Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

THESIS / THÈSE

DOCTEUR EN SCIENCES JURIDIQUES

L'e-Gouvernement et la protection de la vie privée
Légalité, transparence et contrôle

Degrave, Elise

Award date:
2013

Awarding institution:
Universite de Namur

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 03. Jul. 2025

L'E-GOUVERNEMENT ET LA PROTECTION DE LA VIE PRIVÉE

Légalité, transparence et contrôle

Elise Degrave

Préface de Yves Poullet

Collection du CRIDS

larcier

crids
CENTRE DE RECHERCHE INFORMATION DROIT ET SOCIÉTÉ

à Léon le pingouin

Préface

Chère Madame Degrave, chère Elise,

L'heure n'est plus à la question. Je vous en ai posé tant et vous m'en avez posé tant tout au long de cette aventure qu'on nomme thèse. L'heure n'est pas non plus aux conclusions, une thèse ne se conclut jamais, elle ouvre et appelle des prolongements et je sais que ce livre à peine sur la table de votre éditeur, vous noircirez d'autres pages avec le même bonheur pour le lecteur. Non, l'heure est aux félicitations et aux remerciements.

Être promoteur, c'est s'étonner, c'est, à l'aune de l'intelligence de son doctorant, découvrir ses propres limites et accepter, après avoir eu l'illusion de pouvoir mener la barque du disciple, de découvrir progressivement que c'est lui qui vous mène et vous donne la leçon. Telle fut l'aventure de votre thèse, chère Madame Degrave. Ainsi, le choix du sujet me comblait d'aise : il était basé sur une intuition forte – oserais-je dire qu'un colloque parisien sur l'administration électronique me l'avait soufflé – à savoir que le droit administratif avait quelque chose à apprendre du droit de la protection des données et vice-versa. Il était naturel de vous proposer le pari : n'était-ce pas le droit administratif qui vous avait conduit à Namur ? Vous avez accepté ce pari. J'étais donc sûr de mon coup, pouvoir vous 'mener en bateau' sur l'autre rive.

Je déchantais bien vite. Vous inauguriez un autre 'style' de thèse : loin des controverses doctrinales où j'entendais vous cantonner, vous entendiez éprouver sur le terrain la réalité du droit. Vous avez multiplié les lettres adressées aux fonctionnaires : votre redevance TV, vos allocations familiales, votre revenu cadastral, tout était prétexte à enquête. Si ce genre de démarches vous a certainement valu d'être 'fichée' comme une empêcheuse de tourner en rond par les administrations harcelées, voire par la Commission de protection de la vie privée, je dois avouer que la méthode a permis de révéler une grande ineffectivité de nos lois mais, surtout, a autorisé quelques avancées significatives sur le plan des principes. Ainsi, entre autres, la Commission d'accès aux documents administratifs, peut-être épuisée par vos demandes mais surtout convaincue de la justesse de vos arguments, enjoint à la Banque-carrefour de la sécurité sociale de vous remettre, suite à l'exercice de votre droit d'accès, la table de localisation des données qui vous permet de connaître tous les lieux où sont stockées vos données de sécurité sociale, données sur lesquelles elle a prise dans le cadre du fonctionnement du réseau qu'elle assure. Une telle décision donne de ce fait à l'obligation de

transparence sa véritable portée, bien au-delà d'une interprétation restrictive des dispositions de la loi du 8 décembre 1992 établissant le droit d'accès.

Pire, là où je vous proposais une étude doctrinale et, si possible, de droit comparé, là où je vous parlais des pages immortelles écrites par quelques savants confrères sur le concept philosophico-éthico-juridique de *privacy*, vous préfériez vous adonner à la lecture attentive des avis de la Commission de protection de la vie privée, du médiateur, de la Commission d'accès aux documents administratifs. Vous épluchiez les exposés des motifs, les avis du Conseil d'État, les arrêts de la Cour constitutionnelle, voire des articles de presse. Vous remplissiez des cahiers ATOMA de notes à ce propos sans que je ne puisse comprendre le sens de ce puzzle aux pièces éparpillées. Et puis, et puis, il y a eu cet éclair de génie : le chiffre 3, que vous comme moi préférons au chiffre 2 des thèses françaises, vous inspira trois titres à partir des critères de l'État de droit : légalité, transparence, contrôle, ainsi qu'une autre subdivision en trois volets pour chacun de ces trois critères : l'apport du droit constitutionnel et administratif, celui du droit de la protection des données et enfin, celui de la conciliation de ces deux apports. La thèse prenait forme, le puzzle s'ordonnait : la partition pouvait désormais s'écrire.

Quelques mots sur votre art d'écrire : vous écrivez clairement, je veux dire que non seulement votre prose est agréable à lire mais également que le raisonnement se déroule facilement et que vous usez de vos talents pédagogiques, soignant la forme pour la mettre au service du fond. Des conclusions provisoires rythment les sections ; des annotations en retrait du corps du texte exemplifient le propos fort heureusement ; chaque étape du raisonnement fait l'objet d'un numéro et d'un titre. Bref, vous proposez au lecteur un cheminement qui, pas à pas, le conduit agréablement au panorama final.

Au plaisir de la lecture, vous ajoutez celui d'une approche pragmatique : les concepts étudiés sont vus non pour eux-mêmes mais pour les résultats concrets auxquels leur utilisation peut conduire. Le débat que vous entreprenez au Titre III sur la notion d'autorité indépendante et son application à la Commission de protection de la vie privée en est un bel exemple. La finesse de votre raisonnement a pour seule finalité de démontrer la possibilité de recours contre les « décisions » d'une telle « autorité ». Votre souci de répondre aux questions concrètes du citoyen vous amène à ne pas vous contenter de réflexions abstraites mais à exemplifier votre propos et proposer des solutions concrètes de *lege lata* ou de *lege ferenda* parfois inattendues. Ainsi, dans votre Titre III sur le contrôle, vous suggérez des pistes de contrôle juridictionnel qui demeurent jusqu'à présent inexplorées et que l'avocat aura soin de suivre.

Certes, il eût été intéressant, à l'instar d'autres pays, de réfléchir l'e-gouvernement en des termes différents, de suivre l'exemple de la France

qui privilégie un modèle différent où chaque citoyen reçoit des administrations la possibilité de constituer lui-même les pièces de son dossier administratif, en collectant électroniquement tantôt un acte de naissance, tantôt une attestation fiscale de revenus ou tel ou tel document de sécurité sociale. La comparaison de ce modèle étranger d' « *user's (ou de citizen's) empowerment* » et de celui de « *benevolent government* » mis en place par notre pays à travers la constitution de vastes réseaux de transmission des données et dossiers électroniques n'est pas envisagée. Avec raison, vous vous situez résolument dans le système belge où l'électronique est considérée d'abord comme une aide à une action administrative plus efficace qui doit ainsi mieux servir le citoyen. Le législateur belge pourrait trouver dans votre thèse une justification de ses choix : 'source authentique', 'guichet de collecte unique', 'réseaux sectoriels'. Qu'il prenne cependant garde aux balises que vous entendez imposer lorsque vous réclamez la légalité de son action, sa transparence et soumettez celle-là à un contrôle réel.

Votre introduction justifie à plein l'importance du débat qui sous-tend votre thèse : quelle administration électronique voulons-nous ? Le débat s'entame par une réflexion sur les deux pôles de votre recherche. La dimension électronique vous amène à montrer que l'utilisation des technologies de l'information et de la communication révolutionne la structure et l'action de l'administration, là où une administration en silos bien cloisonnés protégeait du *profiling* et du réseautage. La défense de la vie privée justifie votre réflexion sur les limites particulières de ces '*Big Brothers*' publics. Auparavant, le citoyen pouvait s'abriter derrière la relative inefficacité de l'administration. Désormais, l'administration dispose d'informations de qualité et de quantité infiniment meilleures et par ailleurs se vit en réseaux qui multiplient son efficacité et rendent le citoyen transparent. Il est clair que les '*Big Brothers*' ne relèvent plus seulement du secteur privé (Google, Facebook, …) mais également, aujourd'hui, du secteur public qui utilise les mêmes armes à son profit. La vie privée ne se définit pas tant comme un droit de rester à l'abri du regard de l'administration mais plutôt, de manière positive, comme une condition d'exercice des libertés, ce qui implique un minimum d'opacité mais surtout une maîtrise de la circulation de 'son' image informationnelle, la transparence des circuits d'information et donc un contrôle démocratique de ces circuits par le pouvoir législatif et le pouvoir judiciaire. Pour paraphraser Paul Martens : « Ce qui fonde la valeur constitutionnelle de la vie privée, ce n'est ni le droit de tricher, ni le désir mondain de cacher ses richesses ou ses péchés. De tels objectifs peuvent laisser la vie privée retourner sans regret au secteur des manières. Ce que le respect de la vie privée doit empêcher, c'est que l'individu ne devienne transparent aux yeux des pouvoirs publics et privés. Ce n'est pas l'indiscrétion croissante qui est inquiétante, c'est la concentration du pouvoir détenu par ceux qui les regardent

et leur pouvoir non contestable ». Aussi, il est urgent qu'au contrôle individuel largement illusoire du citoyen – contrôle que nos lois de protection des données accordent grâce au consentement, au droit d'accès, au droit de rectification – s'ajoute un contrôle collectif par un véritable débat de tous les acteurs intéressés. Sans doute, ce débat n'est-il rendu possible que par la transparence des circuits d'information et par l'existence d'organes de contrôle réellement indépendants suscitant le débat public, permettant une décision éclairée et, on peut l'espérer, consensuelle entre tous les acteurs.

S'il faut parler d'éthique, c'est bien celle de l'exigence de réseaux au fonctionnement transparent et celle d'un débat public parfaitement informé. La démarche critique vis-à-vis du développement de l'administration électronique est d'autant moins aisée que chacun d'entre nous se réjouit quotidiennement des facilités qu'accorde la mise en place d'une administration électronique bien huilée : l'automaticité des droits, la disparition des tracasseries administratives, etc. Volontiers, des citoyens plaident pour que l'administration, sans doute avec leur accord et parfois avec quelques informations supplémentaires, puisse les profiler afin de leur rendre un meilleur service, voire communiquer leurs données à des entreprises du secteur privé, dans la même perspective. On connaît ainsi la généralisation de l'utilisation de l'e-ID dans le secteur privé comme mode d'authentification lors de transactions privées.

Face à ces dérives, chère Madame Degrave, chère Elise, vous entendez montrer que la conjonction tant des textes en matière de vie privée que de ceux de droit administratif impose des balises à ce développement de l'e-gouvernement. Dans cette démonstration, vous faites preuve de deux qualités proprement universitaires : l'indépendance d'esprit et l'innovation.

À propos de la première, vous n'hésitez pas – et toujours en motivant soigneusement votre propos certes parfois un peu mordant – à critiquer les 'autorités', y compris de la Cour constitutionnelle qui rend 'un arrêt décevant', ou lorsque face à l'intégration, par un arrêté royal que vous jugez illégal, d'une institution qualifiée de sécurité sociale dans le réseau de la Banque-carrefour de sécurité sociale, vous vous étonnez de l'absence de recours devant les juridictions de l'ordre judicaire sur la base de l'article 159 de la Constitution et concluez sévèrement devant ce silence coupable : « c'est probablement la raison pour laquelle de tels arrêtés royaux existent et subsistent ». Bref, vous n'avez pas peur d'exprimer votre opinion y compris en exerçant vous-même des recours concrets et des plaintes devant la Commission de protection de la vie privée et la Commission d'accès aux documents administratifs. La chose est suffisamment rare dans nos milieux universitaires pour que je me plaise à souligner votre courage.

La seconde qualité retiendra encore plus l'attention du lecteur comme elle a retenu celle du jury : votre thèse ose innover. Au fil des pages, votre

thèse révèle un apport considérable dans nombre de domaines du droit. Sans prétendre être exhaustif, j'en relève quelques-uns.

En droit constitutionnel, vous suggérez l'application à l'article 22 de la Constitution de la théorie du « tout indissociable ». Il s'agit d'interpréter l'article 22 de la constitution, non seulement à la lumière de l'article 8 de la Convention européenne des droits de l'Homme et à sa jurisprudence (ainsi, l'arrêt *Rotaru* de la Cour de Strasbourg vous permet de fonder l'obligation de préciser les éléments essentiels du traitement de données dans la loi elle-même), mais également à la lumière aujourd'hui de la directive de l'Union européenne de 1995 traduite par la loi du 8 décembre 1992, demain du règlement européen de protection des données actuellement dans sa phase finale de discussion au Parlement européen. Autre point intéressant, vous défendez de manière convaincante l'obligation constitutionnelle de réévaluer les lois parfois anciennes au regard de la nouvelle donne que constitue l'article 22 de la Constitution. Enfin, les questions délicates, d'une part, de l'échange de données à caractère personnel entre les administrations de l'État fédéral et celles des entités fédérées et, d'autre part, de la répartition des compétences en la matière entre ces différents niveaux de pouvoir, trouvent dans le principe de proportionnalité et la nécessité d'accords de coopération leur solution. Peut-être aurait-il fallu pousser vos conclusions plus loin encore et vous interroger sur le bien-fondé d'autorité de protection des données aux différents niveaux de pouvoir existant dans notre État fédéral ?

C'est au droit administratif que vous réservez une grande partie de vos réflexions innovantes. Ainsi, vous émettez la nécessité de reconnaître des principes généraux nouveaux de l'action administrative dans notre société de l'information : la réciprocité des avantages, qui implique que la technologie facilitant l'action de l'administration puisse également bénéficier au citoyen (accès électronique au dossier, droit de suivi électronique du dossier dans sa circulation au sein des différentes administrations), l'obligation, que vous empruntez aux modèles québécois et hollandais à la fois de répartir les flux informationnels et en même temps de faciliter les échanges de données dans le cadre de réseaux sectoriels et ce, suivant les grands thématiques de la vie administrative des citoyens (le domaine de la sécurité sociale, de la mobilité, de la fiscalité, de la gestion de la population, de l'économie, etc.). Vous estimez qu'il existe un devoir de l'administration d'utiliser au mieux les ressources informatiques pour faciliter la vie des citoyens et de préférer la collecte indirecte à celle directe lorsque la donnée existe déjà au sein de l'administration. Vous développez avec un rare esprit critique la transformation qu'induit l'utilisation des systèmes informatiques sur le droit des citoyens à obtenir une prestation de l'administration, droit autrefois déclenché par une démarche active du premier et qui demain risque de se

transformer en un devoir de l'administration d'octroyer automatiquement le bénéfice de ce droit.

Vos réflexions sur les transformations du droit administratif à l'aune des exigences de la protection des données vous conduisent à plaider pour un éclatement de certains concepts. Ainsi notamment, la notion de 'document' visée par les lois d'accès aux documents administratifs ne se conçoit plus comme le résultat final du processus administratif. Elle s'étend à l'ensemble du processus qui permet sa production, faute sinon de réaliser la transparence attendue, et englobe aujourd'hui les tables de référence utilisées au sein des réseaux sectoriels pour connaître la localisation de toutes les données nécessaires à un traitement, les critères du profilage à la base d'une décision administrative, etc.

Nous terminerons en évoquant la qualité de votre réflexion sur la nature de la Commission de protection des données. Au départ de développements sur la qualité d'autorité administrative de cette institution, vous aboutissez à lui imposer les obligations de transparence et à soumettre ses 'décisions' à la juridiction du Conseil d'État. Avec vous, on ne peut que souligner l'importance de mettre au centre des discussions sur l'avenir de nos libertés, le rôle d'une autorité réellement indépendante qui puisse opérer en toute transparence, soucieuse de créer un débat public plutôt que d'enfermer le débat, et capable de prise de décisions justifiables devant les juridictions de notre État.

Dernier débat que vous ouvrez : celui des rapports entre droit et technologie. La protection des données à caractère personnel et, au-delà, des libertés, suppose que les choix technologiques prennent en compte les exigences de cette protection. Avec vous, nous ne pouvons que nous réjouir de cette alliance du droit et de la technologie que consacrent les principes de '*Privacy by design*' et de *'Privacy Impact Assessment'*. Restent à en définir les contours mais n'est-ce pas là l'objectif que vous vous fixez en acceptant de nourrir la Chaire Droit-Informatique 'E-gouvernement' que notre université vient d'ouvrir ?

Que le combat initié par votre thèse y trouve son prolongement, c'est ce que nous souhaitons à notre jeune docteur pour son plus grand bien et celui de nos citoyens. Merci, chère Madame Degrave, chère Elise, d'avoir rappelé si justement et de continuer à rappeler, au-delà de ce premier chef d'œuvre, que la technologie doit être au service des libertés, de notre démocratie et de l'État de Droit. C'est tout le bonheur que vous souhaite un promoteur fier et heureux.

Yves POULLET
Namur, le 17 septembre 2013

Remerciements

Cet ouvrage est la version remaniée d'une thèse de doctorat défendue publiquement à la Faculté de droit de l'Université de Namur, le 17 mai 2013. Le jury de la thèse était composé du Professeur Yves Poullet, promoteur de la thèse ; du Conseiller d'État David De Roy et du Professeur Cécile de Terwangne, membres du comité d'encadrement de la thèse ainsi que des Professeurs Pierre Trudel, Jean-Jacques Lavenue, Marc Nihoul et Etienne Montero.

Avant cette soutenance publique, nombreux furent les moments où, me sentant perdue face à l'issue encore incertaine de la thèse, j'ai été portée par une envie : celle de pouvoir, un jour, remercier les personnes qui m'ont accompagnée, et surtout supportée, durant ces cinq années de recherche. C'est dire combien je suis heureuse de pouvoir enfin écrire ces lignes, qui désormais leur appartiennent.

Ma reconnaissance va tout d'abord à mon promoteur, le Professeur Yves Poullet. Il a développé des trésors de patience, d'intelligence, d'humour, de tolérance et d'empathie tout au long de mon parcours de doctorante, en particulier s'agissant de mes questions inlassablement répétées jusqu'à obtention d'une réponse convaincante, ce qui m'a d'ailleurs valu le surnom de « Pivert ». Un auteur a dit que « le talent d'un maître se signale non par la docilité de ses élèves mais par leur originalité ». Je ne prétends pas être originale mais je reconnais que je n'ai pas toujours été docile. Je remercie donc mon promoteur de n'avoir jamais essayé de me couler dans un moule de juriste qu'il aurait lui-même défini, ce qui aurait certainement été plus reposant pour lui. Fort de son incroyable intuition, de son expertise, de son ouverture d'esprit et de sa générosité spontanée, il m'a guidée, réagissant avec sagacité à ce que je lui soumettais et m'empêchant de céder à la facilité. Et surtout, il m'a poussée à croire en moi et à écrire une thèse qui serait la mienne. C'est un honneur d'avoir pu franchir cette étape de ma vie professionnelle à ses côtés.

Merci à David De Roy qui a accepté de faire partie du comité d'encadrement de la thèse alors qu'il devenait Conseiller d'État. Erudit, perspicace et généreux, il m'a beaucoup appris. Avec lui, des questions de droit administratif *a priori* décourageantes deviennent passionnantes, au point que, désormais, même la circonscription de la notion d' « autorité administrative » m'enthousiasme.

Merci au Professeur Cécile de Terwangne, également membre du comité d'encadrement de la thèse, pour nos conversations pragmatiques

et stimulantes, son enthousiasme constant durant ce marathon et la confiance indéfectible qu'elle a toujours marquée à l'égard de mon travail.

Merci au Professeur Pierre Trudel, de l'Université de Montréal, au Professeur Jean-Jacques Lavenue, de l'Université de Lille 2, au Professeur Marc Nihoul, de l'Université de Namur, d'avoir accepté de faire partie du jury de la thèse et d'avoir partagé leurs remarques minutieuses et judicieuses. Celles-ci m'ont aidée à enrichir la version publiée de mon travail.

Merci également au Professeur Etienne Montero, Doyen de la Faculté de droit de l'Université de Namur, d'avoir présidé ce jury. Et surtout, avant cela, merci pour la confiance et le respect dont il m'a témoignés durant mes années d'assistanat.

Merci aussi à la Faculté de droit de l'Université de Namur et au Crids. Aux professeurs, aux assistants, aux chercheurs, à l'équipe administrative et à notre informaticien. Ils m'ont entourée et encouragée pendant la thèse. En particulier, merci d'avoir écouté mes réflexions et d'avoir nourri des débats passionnés et passionnants. Merci d'avoir souvent dépanné mon ordinateur, l'imprimante et la machine à café. Merci d'avoir accepté que je garde les livres de la bibliothèque bien plus longtemps que prévu. Merci pour nos boutades et nos fous-rires dans le couloir (moments surnommés « team building »), qui ont été de bonnes respirations entre les chapitres.

Merci à l'équipe du cours de Sources et principes du droit, au sein de laquelle j'ai pu m'investir avec bonheur aux côtés du professeur Yves Poullet, de Karen Rosier et de Franck Dumortier, ainsi qu'à tous ceux et celles qui ont été étudiant(e)s en BAC 1 entre 2006 et 2013. Mêler quotidiennement la pédagogie à la recherche constitua une réelle source d'épanouissement.

Au-delà des murs de la Faculté, j'ai également pu compter sur l'aide et la gentillesse de nombreuses personnes impliquées dans la construction de l'e-gouvernement et le souci de protéger la vie privée. Merci à la Commission de la protection de la vie privée belge, à la *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* allemande, à la Commission nationale pour la protection des données luxembourgeoise, à l'*Agencia de Protección de Datos* espagnole. Merci également aux membres du Centre de recherches en droit public de l'Université de Montréal qui m'ont accueillie pour un séjour de recherches enrichissant, ainsi qu'au Commissariat à la protection des données d'Ottawa et à la Commission d'accès à l'information du Québec, qui ont accepté de me rencontrer longuement. Merci, enfin, aux nombreuses administrations qui ont répondu à mes questions tout aussi nombreuses.

Je ne pourrais clore ces remerciements sans faire une ingérence dans ma vie privée et celle de quelques personnes qui me sont particulièrement chères.

Je remercie mes parents, Jean-Paul et Françoise Degrave-Persoons. L'aboutissement de ma thèse est aussi celui de ma formation universitaire, durant laquelle ils m'ont beaucoup soutenue. Merci à mon papa qui, comme juge de paix, m'a montré que le droit est avant tout un outil au service de causes humaines, ce qui m'a donné l'envie d'étudier cette belle matière. Il est aussi violoniste et, avec lui, j'ai appris le violoncelle. Je lui dois ce cadeau éternel qui est aussi la plus belle des formations, même pour écrire une thèse de doctorat. Merci également à ma maman qui est enseignante depuis trente ans. Une enseignante avec une vraie flamme. Elle m'a transmis le goût de la réflexion fondamentale et de l'effort intellectuel. Elle m'a aussi confié sa passion pour la pédagogie qui désormais m'anime au quotidien.

Merci à mes deux belles « belles-filles », Eléonore et Clémence. Un jour, elles n'ont plus osé me demander si ma thèse avançait. Leur silence a été un réel coup de fouet à mon orgueil et une dose d'adrénaline pour le sprint final.

Elle se cache entre chaque ligne de ce livre. C'est ma fille, Jeanne. Elle a bouleversé ma vie et, dans le même temps, elle l'a structurée. Elle est mon rêve éveillé.

Merci, enfin, à mon amoureux, qui est aussi mon mari, Marc. Il me donne des racines et des ailes. Sans lui, cette thèse … je l'aurais probablement réalisée. Mais il est certain qu'alors, j'aurais perdu l'équilibre. La sérénité que je ressens au moment d'écrire ces lignes, je la lui dois. Et je la lui dédie.

*

Sommaire

Préface **7**

Remerciements **13**

Sommaire **17**

Introduction générale **19**

Prélude **29**

Introduction 31

CHAPITRE I. L'e-gouvernement 33

CHAPITRE II. La protection de la vie privée et des données à caractère personnel 103

Conclusions du prélude 129

Titre I. La légalité de l'e-gouvernement **131**

Introduction 133

CHAPITRE I. L'e-gouvernement et l'exigence constitutionnelle de légalité 135

CHAPITRE II. L'e-gouvernement et les exigences de finalité et de proportionnalité des traitements de données à caractère personnel 177

CHAPITRE III. L'organisation d'un e-gouvernement légal 237

Conclusions du Titre I 309

Titre II. La transparence de l'e-gouvernement **311**

Introduction 313

CHAPITRE I. L'e-gouvernement et la transparence administrative 315

CHAPITRE II. L'e-gouvernement et la transparence des traitements de données à caractère personnel 399

CHAPITRE III. L'organisation d'un e-gouvernement transparent 443

Conclusions du Titre II 475

Titre III. Le contrôle de l'e-gouvernement **477**

Introduction 479

CHAPITRE I. L'e-gouvernement et le contrôle organisé par le droit administratif 481

CHAPITRE II. L'e-gouvernement et le contrôle organisé par le régime juridique de la protection des données à caractère personnel 545

CHAPITRE III. L'organisation d'un e-gouvernement contrôlé 665

Conclusions du Titre III 715

Conclusions générales **717**

Bibliographie **729**

Table des matières **749**

Introduction générale

1.- L'objet de la recherche. L'administration se modernise. Elle recourt de plus en plus souvent aux technologies pour renforcer l'efficacité de son action. À présent, l'administration est entrée dans l'ère de l'*electronic government*, ou « e-gouvernement ». Ce terme générique recouvre l'ensemble des utilisations des technologies de l'information et de la communication dans l'administration, ainsi que les mutations que ces utilisations engendrent au sein de cette dernière[1].

Le présent ouvrage est né du constat que l'informatisation de l'administration n'est pas une simple modernisation technique de l'action administrative. On ne peut pas réduire une base de données à une version actualisée d'un fichier papier, ni considérer qu'un échange électronique de données équivaut à l'envoi de la photocopie d'un document par la poste.

L'informatisation de l'administration a pris un tournant décisif lors de la mise en place du Registre national des personnes physiques en 1983, qui a éveillé chez les citoyens des craintes liées à la protection de leur vie privée dans un État informatisé. Pour la première fois, une réflexion sociétale, prolongée dans les assemblées parlementaires, est alors menée sur le risque de créer un État omniscient qui s'apparenterait au « Big brother » décrit dans le roman de Georges Orwell[2]. Les risques générés par l'informatisation de l'administration sont donc à l'origine des règles de protection des données à caractère personnel consacrées dans la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Quelques années plus tôt, les mêmes craintes étaient d'ailleurs apparues en France alors que l'État envisageait de mettre en place le projet SAFARI[3]. Il s'agissait d'attribuer à chaque citoyen un numéro d'identification unique pour tous les fichiers publics, de manière à faciliter le regroupement de leurs informations. Les vives contestations rencontrées par ce projet ont abouti à l'adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Aujourd'hui, les craintes liées à l'e-gouvernement sont amplifiées par le déploiement considérable des technologies au sein de l'administration. Les outils techniques sont de plus en plus perfectionnés et des interconnexions

---

[1] Nous revenons ultérieurement sur cette définition. Voy. *infra,* n° 8.-

[2] G. Orwell, *1984,* Paris, Gallimard, 1949.

[3] SAFARI est l'acronyme de « système automatisé pour les fichiers administratifs et le répertoire des individus ».

de fichiers sont mises en place. Corollairement à cela, les citoyens sont contraints de divulguer à l'administration des données personnelles multiples et diverses, sous peine de ne pas bénéficier de la prestation demandée ou de ne pas respecter leurs obligations civiques. Outre la mise en place d'un « Big brother », point un autre danger tout aussi fondamental : celui de développer une administration kafkaïenne, c'est-à-dire, une administration à ce point technique et complexe qu'elle en devient incompréhensible et, dès lors, incontrôlable. Comment faire, alors, pour que le citoyen ne soit pas exclu de l'évolution numérique et qu'il garde une prise sur l'administration ? Il importe, à l'heure actuelle, de s'interroger sur la manière de baliser l'utilisation des données personnelles dans l'administration et de donner aux citoyens les moyens de contrôler l'usage qui est fait de leurs informations. Le régime juridique de la protection de la vie privée et des données à caractère personnel doit être confronté à ces impératifs.

Par ailleurs, les menaces que l'informatisation de l'administration fait peser sur la vie privée des citoyens bouleversent l'organisation et le fonctionnement de l'administration et soulèvent des questions de droit administratif, que l'on entend ici comme les règles applicable à l'organisation et au fonctionnement de l'administration, en ce compris les exigences fondamentales du droit constitutionnel. Les règles et les principes généraux qui constituent le droit administratif ont, pour la plupart, été pensés et formulés il y a de nombreuses années, par rapport à l'administration traditionnelle fondée principalement sur l'utilisation du papier. Comment appliquer ce régime juridique à l'heure du déploiement des technologies au sein de l'administration ? La recherche consiste donc à étudier les transformations de l'organisation et du fonctionnement de l'administration et, dès lors, du droit administratif, qui sont induites par le régime juridique de la protection de la vie privée et des données à caractère personnel.

2.- L'originalité de la recherche. L'e-gouvernement n'a pas encore fait l'objet d'une étude scientifique systématique au regard du régime juridique de la protection de la vie privée et du droit administratif. Nous avons néanmoins pu compter sur des réflexions, menées en Belgique et à l'étranger, qui ont été d'une aide singulière pour comprendre certains aspects de l'e-gouvernement[4].

[4] La référence de ces travaux est reprise en bibliographie. En Belgique, il s'agit, principalement, des travaux de l'ICRI (*Interdisciplinary Centre for Law and ICT* de l'Université KU Leuven), et, en particulier, des travaux de Dirk De Bot, qui a notamment consacré un ouvrage à l'étude de certaines questions d'e-gouvernement au regard de la protection de la vie privée. Cécile de Terwangne a rédigé une thèse de doctorat sur la mission publique d'information dans la société de l'information et de nombreuses contributions au sujet de la transparence administrative. David De Roy a consacré nombre d'études à des problématiques

Trois raisons principales expliquent l'originalité, mais également la difficulté, du travail de recherche réalisé.

Tout d'abord, l'e-gouvernement retient rarement l'attention de la doctrine, qu'elle soit belge ou étrangère. De manière générale, les administrativistes ne se penchent pas sur les questions de protection des données, et les spécialistes du droit des technologies ne s'intéressent pas l'administration. Comme si les administrativistes craignaient les ordinateurs, et que les spécialistes des nouvelles technologies se sentaient peu à l'aise dans les méandres du droit administratif. Certains auteurs que nous avons mentionnés précédemment font heureusement figure d'exception, et traitent de questions mêlant le droit administratif et le droit des nouvelles technologies.

Ensuite, le corpus normatif applicable à l'e-gouvernement est éclaté et manque de cohérence. Il est également lacunaire. Les normes en la matière se multiplient et sont adoptées au fur et à mesure de la mise en place des outils techniques. Coexistent ainsi une loi sur le Registre national, une loi sur la Banque-Carrefour de la sécurité sociale, une loi sur la Banque-carrefour des entreprises, une loi sur l'intégrateur de service au niveau fédéral, une loi sur le Banque-Carrefour des véhicules, etc. Chacune de ces lois organise l'outil en question, tout en prévoyant des règles particulières concernant la protection des données traitées, qui s'apparentent ou diffèrent des dispositions consacrées par la loi du 8 décembre 1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel. Il est donc difficile d'avoir une vue d'ensemble des règles applicables à l'e-gouvernement et de définir des principes communs à toutes les administrations. De plus, les concepts juridiques qualifiant ces outils sont bien souvent inédits et imposent une étude approfondie des normes mais également de la réalité

---

touchant à l'e-gouvernement, qui concernent notamment la responsabilité et la publicité de l'administration informatisée, ainsi que les autorités administratives indépendantes. Yves Poullet a consacré de nombreux travaux à la protection de la vie privée et des données à caractère personnel en général et, en particulier, à la notion d'autodétermination informationnelle, aux risques liés à certains traitements de données comme le profilage, au principe de réciprocité des avantages, et aux autorités de protection des données. À l'étranger, l'e-gouvernement a retenu l'attention de Georges Chatillon qui a dirigé deux colloques consacrés à l'administration électronique, qui ont chacun donné lieu chacun à un ouvrage, tout comme Jean-Jacques Lavenue qui a notamment dirigé plusieurs colloques consacrés à des questions de droit public en lien avec les technologies. Les contributions d'Herbert Burket et Daniel Solove ont aidé à comprendre les dangers de l'e-gouvernement et à interpréter la notion d'autodétermination informationnelle. Rosario Duaso Cales a récemment rédigé une thèse de doctorat consacrée au principe de finalité et la protection des renseignements personnels dans le secteur public. Enfin, Pierre Trudel a rédigé de nombreuses études sur la protection des données à caractère personnel et des questions de droit public. Ses réflexions sur le modèle de l'État en réseau nous ont été particulièrement utiles.

de terrain pour en comprendre l'exacte portée et proposer des définitions. Par ailleurs, l'étude des normes applicables à l'e-gouvernement suppose également de tenir compte de l'interprétation qu'en donnent différentes instances. S'agissant de l'interprétation des règles de droit européen, les avis de l'organe consultatif européen sur la protection des données et la vie privée, dit « Groupe 29 », ont retenu notre attention. En droit belge, on a analysé les avis de la section de législation du Conseil d'État, mais également les avis de la Commission de la protection de la vie privée, touchant de près ou de loin à l'e-gouvernement. Des avis de la Commission d'accès aux documents administratifs ont également été analysés à l'occasion de l'étude de la transparence de l'e-gouvernement. Par souci de simplification dans la suite de la recherche, nous parlerons de la « jurisprudence » de la section de législation du Conseil d'État, de la « jurisprudence » de la Commission de la protection de la vie privée (« CPVP ») et de la « jurisprudence » de la Commission d'accès aux documents administratifs (« CADA »).

Enfin, rares sont les décisions des cours et tribunaux rendues en matière d'e-gouvernement. Il semble que maintes violations de la protection des données ne soient pas dénoncées en justice, probablement parce que ces règles particulières sont encore trop peu connues des magistrats, des avocats et des citoyens. Néanmoins, la Cour constitutionnelle et le Conseil d'État, section du contentieux administratif, ont eu quelques occasions de se prononcer en cette matière, tout comme certaines juridictions judiciaires. Ces décisions ont retenu toute notre attention.

3.- Les limites de la recherche. La recherche se limite à l'étude de l'e-gouvernement belge. Les solutions appliquées à l'étranger sont néanmoins étudiées lorsqu'elles peuvent inspirer l'organisation de l'e-gouvernement en Belgique. On analyse également la proposition de règlement européen sur la protection des données[5], qui devrait être adoptée prochainement par le Parlement et le Conseil européens, spécialement lorsque les dispositions de ce règlement confirment les solutions belges ou, au contraire, imposent de repenser ces dernières. En outre, nous nous concentrons sur l'e-gouvernement tel qu'il est organisé au niveau fédéral et, en particulier, au sein des services publics fédéraux et de certains organismes de sécurité sociale. Des développements sont néanmoins consacrés aux communautés et aux régions mais uniquement en ce qui concerne la question de la compétence de ces collectivités politiques pour adopter des

[5] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personne physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final.

normes encadrant l'e-gouvernement. Par ailleurs, compte tenu de l'ampleur de la recherche, nous avons exclu de l'objet de notre recherche la problématique spécifique des partenariats publics-privés.

Le corpus normatif étudié dans la recherche est également limité. Nous nous concentrons sur les règles générales du régime juridique de la protection de la vie privée et des données à caractère personnel. Nous n'étudions pas les règles applicables aux traitements de données sensibles[6], ni les règles qui concernent le transfert de données vers des pays non membres de l'Union européenne[7]. Nous n'étudions pas non plus les règles applicables aux traitements de données menés à des fins historiques, statistiques ou scientifiques[8]. Quant au droit administratif, il est abordé principalement au travers des règles organisant la légalité, la transparence et le contrôle de l'administration, pour les raisons exposées ci-après[9].

Peu nombreuses, les décisions des cours et tribunaux ont été étudiées lorsqu'elles ont pour objet l'application, à une administration, du régime juridique de la protection de la vie privée et des données à caractère personnel. Les avis de la Commission de la protection de la vie privée en matière d'e-gouvernement sont beaucoup plus nombreux. Ils ont été analysés pour la période qui s'étend de 1992 à 2012. Il en va de même des avis de la section de législation du Conseil d'État et, au niveau européen, des avis du « Groupe 29 ». Les avis de la Commission d'accès aux documents administratifs n'ont pas été analysés de manière systématique ; seuls les avis permettant d'éclairer certaines notions importantes du régime de la transparence administrative[10] ainsi que les rares avis relatifs à l'e-gouvernement ont été analysés.

4.- L'hypothèse de la recherche. Cet ouvrage entend démontrer qu'il est possible d'organiser un e-gouvernement efficace tout en permettant au citoyen de garder une prise sur l'administration, pour la comprendre et la contrôler. Ce faisant, tant l'efficacité administrative que la protection de la vie privée des citoyens peuvent être assurés.

---

[6] Art. 6 à 8 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après « loi du 8 décembre 1992 »). Il s'agit des données relatives à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que le traitement des données relatives à la vie sexuelle (art. 6). Il s'agit également des données relatives à la santé (art. 7) et des données relatives à des litiges soumis aux cours et tribunaux (art. 8).

[7] Art. 21 et 22 de la loi du 8 décembre 1992.

[8] Art. 4, 2°, de la loi du 8 décembre 1992.

[9] Voy. *infra,* n° 4.-

[10] Ce régime est analysé dans le deuxième chapitre du deuxième titre de la recherche consacré à la transparence de l'e-gouvernement.

Afin d'atteindre ce double objectif, il importe de créer un corpus normatif cohérent pour l'e-gouvernement, fondé sur une articulation délicate entre le droit administratif et le régime juridique de la protection de la vie privée et des données à caractère personnel. Ainsi, la recherche montre que les règles de protection de la vie privée et des données à caractère personnel peuvent être greffées sur le droit administratif, qui s'en trouve ainsi profondément modifié et enrichi. La recherche insiste également sur le fait que des solutions nouvelles doivent être créées pour contrer les dangers de l'e-gouvernement.

Afin de définir la structure qui serait suivie pour effectuer cette démonstration, nous sommes partis du constat que les dangers de l'e-gouvernement pour la protection de la vie privée des citoyens peuvent être classés en trois catégories. Certains dangers concernent les normes applicables à l'e-gouvernement. D'autres risques touchent à la transparence de l'e-gouvernement. Enfin, le contrôle de l'e-gouvernement pose également de nombreuses questions. Nous avons ensuite identifié un lien entre ces risques et les exigences fondamentales du droit administratif, de manière à démontrer en quoi les risques de l'e-gouvernement ébranlent le droit administratif. Le principe de l'État de droit a retenu notre attention[11]. Ce principe impose des exigences qui balisent l'action administrative, et dans lesquelles s'enracine le droit administratif. Il fait l'objet d'une littérature foisonnante de laquelle il apparaît que, si cette notion est « floue et à géométrie variable »[12], se présentant « comme un faisceau de sous-principes […] écrits ou non, et eux-mêmes subdivisés en règles plus particulières »[13], il reste que, s'agissant des conséquences de ce principe sur la structure et le fonctionnement de l'administration, au moins trois exigences sont régulièrement soulignées par la doctrine[14]. Notre démonstration s'effectue au travers de ces trois exigences.

---

[11] L'État de droit peut être défini comme « un État qui, dans ses rapports avec ses sujets et pour la garantie de leur statut individuel, se soumet lui-même à un régime de droit, et cela en tant qu'il enchaîne son action sur eux par des règles dont les unes déterminent les droits réservés aux citoyens, dont les autres fixent par avance les voies et moyens qui pourront être employés en vue de réaliser les buts étatiques ». (R. Carré de Malberg, *Contribution à la théorie générale de l'État,* Paris, 1922, t. I, p. 293).

[12] J. Chevallier, « Avant-propos », *in L'État de droit,* Paris, La Documentation française, 2004, p. 13.

[13] O. Jouanjan, « État de droit », *in Dictionnaire de la culture juridique* (dir. D. Alland et S. Rials), Paris, P.U.F., 2003, p. 650.

[14] Parmi la doctrine abondante sur le sujet, voy. les contributions significatives de J. Chevallier, « Avant-propos », *in L'État de droit,* Paris, La Documentation française, 2004, pp. 5 à 13 ; L. Heuschling, « État de droit. Étude de linguistique, de théorie et de dogmatique juridiques comparées », *in Verfassungsprinzipien in Europa, Constitutional principles in Europa, Principes constitutionnels en Europe* (H. Bauer et C. Callies éd.), Athènes, Berlin,

La première exigence est la *légalité*, c'est-à-dire la soumission des organes de l'État aux règles de droit. Cette exigence empêche l'arbitraire étatique[15] et garantit aux particuliers « d'être conduits non par le bon plaisir individuel des gouvernants et des fonctionnaires, mais par des règles objectives que fixent, dans l'intérêt général, des autorités qui peuvent être appelées à rendre compte de leurs actes »[16].

La deuxième exigence est la *transparence*. Il s'agit d'une valeur incitant l'administration à appliquer les règles de droit de manière équitable et raisonnable ou, pour le dire autrement, de manière impartiale et sage. Elle se décline en plusieurs obligations précises qui s'imposent aux administrations dans l'exercice de leurs missions.

La troisième exigence est le *contrôle* des institutions. Elle garantit la soumission des autorités publiques aux règles de droit et assure ainsi l'effectivité de ces dernières.

5.- La méthode de la recherche. Cette recherche fondamentale est animée, depuis l'origine, du souci de nourrir la matière de perspectives réalistes, qui tiennent compte du contexte dans lequel s'inscrivent actuellement l'organisation et le fonctionnement de l'administration belge. On a souhaité proposer des solutions raisonnablement envisageables et qui pourront, on l'espère, éclairer utilement les législateurs, les administrations et les citoyens, dans ce domaine du droit en pleine évolution. Ce souci de réalisme se marque principalement à trois égards.

Premièrement, nos réflexions sont fondées sur une démarche initialement empirique, qui a été menée durant les premiers mois de la recherche. Elle a consisté à tester, effectivement, les prérogatives que les citoyens peuvent faire valoir à l'égard de l'administration, et qui sont organisées par le régime juridique de la protection de la vie privée et des données à caractère personnel ainsi que par le droit administratif. Concrètement, nous avons écrit à diverses administrations pour exercer nos droits, en tant que citoyenne belge. Nous avons ainsi invoqué des règles de droit administratif pour demander l'accès à certains documents administratifs pertinents dans le contexte de l'e-gouvernement.

Bruxelles, Ant. N. Sakkoulas, Berliner wissenschaft-verlag, Bruylant, 2008, pp. 103 à 155 ; M. Verdussen, « La signification du principe de l'État de droit pour l'administration en Europe », *op. cit.,* pp. 189 à 218 ; Ph. Quertainmont, « Le déclin de l'État de droit », *J.T.,* 1984, pp. 273 à 280.

[15] F. Delpérée, *Le droit constitutionnel de la Belgique,* Bruxelles, Bruylant, Paris, L.G.D.J., 2000, p. 95.

[16] A. Molitor, *L'administration publique,* Paris, Unesco, 1958, p. 92 cité par Ph. Quertainmont, « Le déclin de l'État de droit », *J.T.,* 1984, p. 273.

Nous avons également mobilisé les règles de protection des données pour obtenir des administrations qu'elles nous livrent les informations relatives aux données à caractère personnel qu'elles détiennent à notre sujet. À plusieurs reprises, des agents de l'administration ont ensuite pris contact avec nous par téléphone pour nous faire part des difficultés qu'ils rencontraient pour répondre à notre demande. Nous avons ainsi pu constater, notamment, que les règles applicables à l'e-gouvernement et, en particulier, les règles de protection des données, sont peu connues au sein de l'administration, notamment parce que rares sont les citoyens qui font valoir leurs droits en cette matière. Dans certaines administrations, notre demande d'accéder à nos données à caractère personnel était la première demande de ce type, alors que ce droit existe depuis 1992. Par ailleurs, nous avons également exercé des recours lorsque la réponse de certaines administrations nous paraissait critiquable. C'est la raison pour laquelle, à deux reprises, nous avons sollicité l'avis de la Commission d'accès aux documents administratifs. Ces démarches ont utilement éclairé les forces et les lacunes des règles qui entourent l'e-gouvernement et ont ensuite nourri et guidé nos réflexions théoriques.

Deuxièmement, le souci de réalisme se marque également dans les solutions proposées. Nous avons choisi d'inscrire nos réflexions dans le prolongement des outils technologiques déjà mis en place au sein de l'administration belge. Ainsi, notamment, on a choisi, en Belgique, d'organiser une circulation maximale des données entre les administrations, de manière à ne pas devoir contacter le citoyen pour obtenir les informations nécessaires. Cela s'est concrétisé par exemple, par la mise en place de la Banque-carrefour de la sécurité sociale en 1995. Nous n'ignorons pas que d'autres modèles d'e-gouvernement sont envisageables. Néanmoins, dans la mesure où notre administration est engagée dans un modèle de ce type, nous n'avons pas élaboré de solutions qui impliqueraient un changement de cap fondamental, voire un anéantissement des outils déjà fonctionnels au sein de l'administration. Le souci de réalisme se double de la volonté d'être pragmatique et utile. C'est pourquoi, au-delà des réflexions théoriques présentées, nous proposons des solutions concrètes qui pourraient être reprises par le législateur, comme le montrent notamment les développements relatifs à l'élaboration d'une loi-cadre pour l'e-gouvernement.

Troisièmement, tout au long de la recherche, nous illustrons nos réflexions par des exemples, de manière à montrer l'incidence concrète des développements théoriques. De nombreux exemples sont tirés de la jurisprudence foisonnante de la Commission de la protection de la vie privée. D'autres ont été construits. Des extraits de jurisprudence sont également repris *in extenso* pour illustrer l'application, par les juridictions, des règles étudiées. Régulièrement, nous mettons également en évidence des

extraits d'avis de la section de législation du Conseil d'État et de la Commission de la protection de la vie privée, ces avis étant utiles pour éclairer les normes applicables à l'e-gouvernement, nombre d'entre elles étant particulièrement floues. De manière générale, ces exemples et ces extraits de jurisprudence sont repris dans un paragraphe centré et écrit en plus petits caractères, tout comme les dispositions normatives commentées et les extraits des travaux parlementaires cités.

6.- Le plan de la recherche. La recherche est divisée en trois titres, chacun étant orienté sur une exigence fondamentale de l'État de droit à partir de laquelle s'effectue la démonstration. Le premier titre est consacré à la légalité de l'e-gouvernement, le deuxième titre à la transparence de l'e-gouvernement et le troisième titre au contrôle de l'e-gouvernement. Pour chaque titre, on montre, dans un premier chapitre, comment le droit administratif organise l'exigence étudiée. On précise, dans un deuxième chapitre, en quoi le régime juridique de la protection de la vie privée et des données à caractère personnel répond à la même exigence tout en enrichissant le droit administratif. On suggère, dans un troisième chapitre, des solutions pour adapter l'ensemble de ces règles aux enjeux de l'e-gouvernement de manière à ce que l'exigence en question soit respectée et que le citoyen garde une prise sur l'administration dans ce contexte nouveau.

Ces trois titres sont précédés d'un prélude consacré aux notions cardinales de l'e-gouvernement et du régime juridique de la protection de la vie privée et des données à caractère personnel. L'e-gouvernement est fondé sur des outils techniques dont il sera question à maintes reprises dans les développements ultérieurs. Il nous a donc paru nécessaire d'expliquer, de définir et d'illustrer par des exemples concrets ces moyens nouveaux dont dispose l'administration. De plus, l'e-gouvernement génère des risques, plus ou moins évidents. Ils sont circonscrits et mis en lumière. La deuxième partie du prélude est consacrée au régime juridique de la protection de la vie privée et des données à caractère personnel, étant donné que ces règles sont encore trop peu connues et mal comprises, que ce soit parmi les juristes en général ou les administrations en particulier. La raison d'être de ce régime juridique particulier est expliquée et les normes qui le composent sont exposées. Enfin, nous expliquons les éléments principaux sur lesquels se fonde le régime juridique de la protection de la vie privée et des données à caractère personnel.

* * *

Prélude

Introduction

7.- Les prolégomènes. Bien souvent, la compréhension d'une matière qui implique l'usage des technologies suppose la maîtrise de réalités nouvelles, de concepts inédits et de normes particulières. L'étude de l'e-gouvernement n'échappe pas à la règle.

C'est pourquoi, cette partie de la recherche, écrite en guise de prélude à l'ouvrage, pose les jalons techniques et conceptuels qui ouvrent aux développements juridiques formant les trois titres de la présente recherche doctorale, dédiés à la légalité, à la transparence et au contrôle de l'e-gouvernement.

La première partie du prélude est consacrée à la réalité de l'e-gouvernement. Les outils techniques dont dispose aujourd'hui l'administration sont décrits, définis et illustrés par des exemples concrets. Leurs applications sont analysées. Nous clarifions ensuite les risques générés par l'e-gouvernement, car ils guideront nos réflexions juridiques et les solutions proposées au terme de notre démonstration.

Dans la deuxième partie de ce prélude, les traits saillants de la protection de la vie privée et des données à caractère personnel sont esquissés. Ce régime juridique particulier est, à maints égards, difficile à appréhender. Dès lors, nous expliquons sa raison d'être, en développant notamment le lien entre la protection des données à caractère personnel et le droit fondamental à la vie privée. Ensuite, nous détaillons les normes et les notions principales sur lesquelles se fonde ce régime juridique.

* * *

CHAPITRE I.
L'e-gouvernement

Introduction

8.- La définition de l'e-gouvernement. L'e-gouvernement, appelé aussi « electronic government » ou « administration électronique », est un terme générique qui recouvre l'ensemble des utilisations des technologies de l'information et de la communication dans l'administration, ainsi que les mutations que ces utilisations engendrent au sein de cette dernière[17].

Ces changements concernent, d'une part, le *back office* de l'administration, c'est-à-dire sa structure et son fonctionnement internes. Comme nous le détaillerons par la suite, il y a quelques années, l'administration se présentait comme une multiplication de ministères séparés, cloisonnés, travaillant chacun de leur côté en collectant les informations dont ils avaient besoin. Chaque ministère constituait « une administration autonome »[18], un « tout fonctionnellement et organiquement structuré »[19]. À

[17] Cette définition comporte les éléments les plus pertinents mentionnés dans différentes descriptions de l'e-gouvernement reprises dans les documents suivants : Commission des Communautés européennes, « Le rôle de l'administration en ligne (eGovernment) pour l'avenir de l'Europe », COM(2003) 567 final, du 26 septembre 2003, p. 4 ; Commission des Communautés européennes, « L'information émanant du secteur public : une ressource clef pour l'Europe. Livre vert sur l'information émanant du secteur public dans la société de l'information », COM(1998)585, p. 8 ; Observatoire des Droits de l'Internet, « Facteurs de succès de l'e-gouvernement. Avis n° 2 », décembre 2003, disponible sur le site http://www.internet-observatory.be ; Banque mondiale, « Definition of E-Government », http://web.worldbank.org ; R. Silcock, « What is e-government ? », *Parliamentary Affairs,* 2001, vol. 54, p. 88 ; D. De Roy, C. de Terwangne et Y. Poullet, « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », *C.D.P.K.,* 2007, p. 310 ; E. Boudry, F. De Rynck, S. Janssens et S. Rotthier, *E-government : nieuwe kans of nieuw probleem,* Brugge, die Keure, 2009, pp. 1 et 2 ; G. Chatillon, « Fondements, principes et nature du droit de l'administration électronique », *in Droit de l'administration électronique. De nouveaux droits pour les usagers. Des nouvelles règles pour les agents* (dir. G. Chatillon), Bruxelles, Bruylant, 2011, pp. 28 et 29 ; P. Trudel, « Existe-t-il un droit public de la gouvernance en ligne ? », *op. cit.,* p. 312 ; F. Bundshuch-Rieseneder, « Governance and e-governance in the frame of Bologna Process », *in Bologna Process, European Construction, European Neighbourhood Policy* (dir. T. Come et G. Rouet), Bruxelles, Bruylant, 2011, p. 260.

[18] R. Wilkin, *L'administration publique belge,* Bruxelles, Bruylant, 1958, p. 34.

[19] C. Cambier, *Droit administratif,* Bruxelles, Larcier, 1968, p. 26.

la tête du ministère se trouvait un ministre administrant « seul son département sans en référer aux collègues »[20].

L'e-gouvernement modifie profondément cette structure. On assiste notamment à la création de réseaux sectoriels qui regroupent chacun plusieurs administrations ayant un domaine d'action en commun. Le fonctionnement de l'administration connaît également des changements. Plutôt que de collecter toutes les mêmes informations à répétition, on charge les administrations de collecter et de mettre à jour un nombre limité d'informations déterminées. Ces informations seront ensuite échangées, par voie informatique, entre les institutions qui en ont besoin.

D'autre part, l'e-gouvernement provoque des changements au niveau du « *front office* » de l'administration, à savoir, les services rendus par l'administration au citoyen. Grâce aux technologies, on est en mesure de simplifier les démarches administratives. Entre autres exemples, l'e-gouvernement permet au citoyen de remplir sa déclaration fiscale en ligne, grâce au système *Tax-on-web*. L'utilisation d'internet rend possible la publication, en ligne, de nombreuses informations administratives. La mise en place de « guichets uniques » facilite les démarches du citoyen en l'orientant vers un interlocuteur qui se charge de tâches pour lesquelles le citoyen devait jadis contacter plusieurs instances différentes. Cet interlocuteur peut être chargé de missions diverses, telles que transmettre la demande au service compétent, constituer le dossier de la personne, fournir des conseils, etc.[21].

Concrètement, des liens évidents existent entre le *back office* et le *front office* de l'administration. Par exemple, la déclaration d'impôts accessible en ligne grâce au système *Tax-on-web* contient des données pré-encodées, parce que, en amont, dans le *back office*, des échanges de données ont été effectués entre certaines administrations et le SPF Finances. À l'inverse, les modifications opérées dans l'organisation et le fonctionnement de l'administration doivent tenir compte des difficultés rencontrées dans les relations entre l'administration et le citoyen, au niveau du *front office*.

Notre recherche se concentre principalement sur l'étude du *back office* de l'administration. Nous n'ignorons toutefois pas l'impact des questions étudiées sur le *front office*, qui sera d'ailleurs évoqué, principalement dans le chapitre consacré à la transparence de l'e-gouvernement.

---

[20] R. Wilkin, *op. cit.*, p. 34.

[21] Actuellement, les principaux guichets uniques mis en place sont dédiés aux démarches administratives des entreprises. Voy. les art. 42 et s. de la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des entreprises, modernisation du registre du commerce, création d'enreprises agréés et portant dispositions diverses.

9.- La raison d'être de l'e-gouvernement. L'e-gouvernement est motivé par la volonté de renforcer l'efficacité de l'administration tout en facilitant les démarches administratives des citoyens.

Pour les pouvoirs publics, les technologies, non seulement, constituent un moyen efficace pour traiter les dossiers de manière plus rapide et plus économique, mais elles offrent également des potentialités sans précédents pour assurer le respect des normes, notamment en permettant de cibler les fraudeurs grâce à de puissants logiciels de calculs ou en rendant possible l'octroi automatique aux plus faibles des bénéfices auxquels ils ont droit.

Pour le citoyen, l'utilisation des technologies dans l'administration est source de confort. Aujourd'hui, un billet d'avion pour faire le tour du monde s'achète en quelques « clics » depuis son ordinateur et à n'importe quel moment, alors que l'obtention d'un document administratif suppose bien souvent que l'on se déplace à l'administration en se soumettant à des horaires contraignants et en fournissant moult documents. L'e-gouvernement permet d'atténuer bien des agacements de ce genre.

En Belgique, l'e-gouvernement prend son essor avec la création du Registre national, qui a eu lieu officieusement dès 1968 avant d'être encadrée légalement par la loi du 8 août 1983 organisant un registre national des personnes physiques[22]. Depuis lors, encouragée par le succès du Registre national et les progrès effectués dans le domaine des technologies de l'information et de la communication, la Belgique s'engage, particulièrement depuis la fin des années nonante, dans le développement substantiel de l'e-gouvernement, répondant ainsi au besoin de moderniser l'État, dans le but d'améliorer le fonctionnement des autorités publiques et, par là, de restaurer la confiance du citoyen en ses institutions[23].

---

[22] *M.B.,* 21 avril 1984.

[23] Accord de gouvernement du 7 juillet 1999 « La voie du XXIème siècle » ; Accord de coopération du 23 mars 2011 entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire flamande, la Commission communautaire française et la Commission communautaire commune concernant la construction et l'exploitation d'une e-plate-forme commune, *M.B.,* 8 août 2001 ; Note stratégique du Secrétaire d'État à l'Informatisation de l'État, Peter Vanvelthoven, Novembre 2003, p. 13 ; Accord de coopération du 28 septembre 2006 entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire française et la Commission communautaire commune concernant les principes pour un e-gouvernement intégré et la construction, l'utilisation et la gestion de développements et de services d'un e-gouvernement intégré, *M.B.,* 19 octobre 2006 ; Accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe

Ce faisant, la Belgique répond pleinement à l'ambition européenne selon laquelle, d'ici 2015, les administrations publiques européennes seront « ouvertes, souples et collaboratives dans leurs relations avec les particuliers et les entreprises. Elles [utiliseront] l'administration en ligne pour accroître leurs performances et leur efficacité et pour améliorer continuellement les services publics de façon à répondre aux différents besoins de l'utilisateur et à maximiser l'utilité publique, facilitant ainsi la transformation de l'Europe en une économie de la connaissance de premier plan »[24].

10.- L'objectif de l'e-gouvernement : la collecte unique des données. Avant le développement de l'e-gouvernement, l'administration était structurée « en silos »[25], ce qui signifie qu'elle était composée de ministères distincts et cloisonnés. Chacun gérait ses propres données, et ses propres moyens de les traiter. Les échanges de données entre ces ministères étaient rares. Ainsi, lors des débats parlementaires relatifs au projet de loi relative à l'informatique, aux fichiers et aux libertés en France, a-t-on mis en évidence « le cloisonnement des administrations et le peu de goût que celles-ci ont à l'ordinaire pour se communiquer les données qu'elles détiennent comme des trésors précieux. L'informatique, par le moyen des interconnexions, rend fluide et automatique la circulation des informations »[26]. Le même constat pouvait être fait en Belgique.

Le développement de l'e-gouvernement rompt radicalement avec ce type de structure administrative. Il est guidé par un objectif à atteindre, la collecte unique des données[27], qui est rendue possible grâce à l'informatique.

---

de cette initiative, *M.B.,* 23 juillet 2013 ; Accord de coopération du 26 août 2013 entre les administrations fédérales, régionales et communautaires afin d'harmoniser et aligner les initiatives visant à réaliser un e-gouvernement intégré, *M.B.,* 8 octobre 2013.

[24] Commission européenne, Plan d'action européen 2011-2015 pour l'administration en ligne « Exploiter les TIC pour promouvoir une administration intelligente, durable et innovante », COM(2010) 743, p. 4.

[25] D. De Roy, C. de Terwangne et Y. Poullet, *op. cit.*, p. 309. Voy. égal. F. Bundshuch-Rieseneder, « Governance and e-governance in the frame of Bologna Process », *in Bologna Process, European Construction, European Neighbourhood Policy* (T. Come et G. Rouet), Bruxelles, Bruylant, 2011, pp. 253 et 254 ; H. Maisl, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », *in L'administration électronique au service des citoyens* (dir. G. Chatillon et B. du Marais), Bruxelles, Bruylant, 2003, pp. 349 à 359 ; R. Duaso Calès, *Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau*, thèse présentée à l'Université de Montréal et à l'Université Panthéon – Assas Paris II, septembre 2011, pp. 37 à 44.

[26] Assemblée nationale (France), Première session ordinaire de 1977-1978, Compte-rendu intégral 2e séance, 4 octobre 1977, Débats relatifs au projet de loi Informatique et Libertés, p. 5782.

[27] Art. 2 de l'Accord de coopération du 28 septembre 2006, précité ; Commission européenne, Plan d'action européen 2011-2015 pour l'administration en ligne « Exploiter les TIC pour promouvoir une administration intelligente, durable et innovante », *op. cit.*, p. 13.

Ce principe consiste à ne demander qu'une seule fois aux citoyens les informations qui les concernent, à la différence de ce qui se faisait dans l'administration traditionnelle où les individus devaient souvent communiquer leurs données à chaque administration avec laquelle ils étaient en contact. En d'autres termes, dès que le citoyen a communiqué une information d'un certain type à une administration, les autres administrations ne peuvent plus la lui réclamer à nouveau.

La collecte unique doit être soutenue par l'organisation de la réutilisation des données entre les administrations. De cette manière, l'institution qui a collecté l'information auprès du citoyen, pourra ensuite la communiquer aux institutions qui en ont besoin, sans méconnaître le principe de la collecte unique.

C'est pourquoi, la structure et le fonctionnement de l'administration sont aujourd'hui repensés pour assurer la collecte unique des données et la réutilisation des informations entre les administrations[28]. Ces deux impératifs sont d'ailleurs officiellement consacrés par la Charte pour une administration à l'écoute des usagers, approuvée par le Conseil des ministres le 23 juin 2006, qui, en son point 12, affirme que « tout service public utilisera de façon optimale les données déjà disponibles auprès d'autres organismes publics ». En outre, l'accord de coopération du 28 septembre 2006 entre l'État fédéral et les entités fédérées concernant l'e-gouvernement[29] érige la collecte unique en principe d'un e-gouvernement intégré et prévoit, en son article 2, que « les Parties reconnaissent que la réalisation d'un e-gouvernement intégré n'est possible que pour autant que les Parties essaient de réaliser les initiatives et projets d'e-gouvernement communs sur la base des principes suivants : […] 2. La collecte unique et la réutilisation maximale de données en utilisant des sources authentiques de données ».

Désormais engagée dans l'ère de l'e-gouvernement, l'administration dispose de techniques nouvelles pour accomplir ses missions. Ces avancées suscitent beaucoup d'enthousiasme. Néanmoins, elles génèrent également certaines craintes auxquelles il convient d'être attentif.

Les lignes qui suivent sont consacrées à ces nouvelles techniques et ces nouvelles craintes. Elles décrivent et illustrent les notions nécessaires pour comprendre les développements ultérieurs[30].

---

[28] Il convient bien évidemment de repenser la structure et le fonctionnement de l'administration également au regard des règles de protection de la vie privée et des données à caractère personnel, ce qui est expliqué dans le deuxième chapitre de ce prélude.

[29] Accord de coopération du 28 septembre 2006, précité.

[30] C'est volontairement que nous ne soulignons pas, à ce stade de la recherche, les problèmes que les nouvelles techniques et les nouvelles craintes soulèvent par rapport aux exigences de la protection de la vie privée des citoyens. Il nous semblerait prématuré de

Section 1. Des techniques nouvelles

11.- De nouveaux outils et de nouvelles opérations. Grâce aux technologies de l'information et de la communication, de nouveaux outils sont mis au service de l'administration et permettent à cette dernière d'effectuer de nouvelles opérations.

I. De nouveaux outils

12.- Réseau sectoriel, source authentique de données, plateforme d'échanges d'information et numéro d'identification. L'e-gouvernement belge se caractérise par la mise en place de réseaux sectoriels au sein de l'administration.

Chaque réseau sectoriel est un ensemble de plusieurs administrations ayant un domaine d'action commun – la sécurité sociale, la santé, les véhicules, etc. – au cœur duquel on place une plateforme d'échanges d'informations. Cette plateforme est chargée d'assurer la circulation des données au sein des administrations du réseau sectoriel, en se servant d'un numéro unique pour identifier chaque citoyen.

Les données qui circulent émanent de sources authentiques de données, qui sont des bases de données particulièrement fiables. Ces sources authentiques de données sont placées dans tout ou partie des administrations du réseau sectoriel.

Cette architecture nouvelle de l'administration est encore peu connue, d'autant plus qu'elle est propre à la Belgique[31]. C'est pourquoi, cette section est consacrée à définir ces outils nouveaux et à les illustrer par des exemples concrets. Afin de faciliter la compréhension de l'exposé, on peut, d'ores et déjà, schématiser comme suit le modèle que constitue le réseau sectoriel et qui est expliqué dans les lignes qui suivent.

souligner ces problèmes sans avoir, au préalable, expliqué et détaillé les exigences juridiques qui s'appliquent à l'e-gouvernement. La confrontation de l'e-gouvernement aux règles de la protection de la vie privée est dès lors étudiée de manière détaillée dans les trois titres qui forment la thèse (légalité, transparence et contrôle).

[31] À notre connaissance, aucun autre État n'a mis en place tant des réseaux sectoriels que des plateformes d'échanges d'informations et des sources authentiques de données dans son administration.

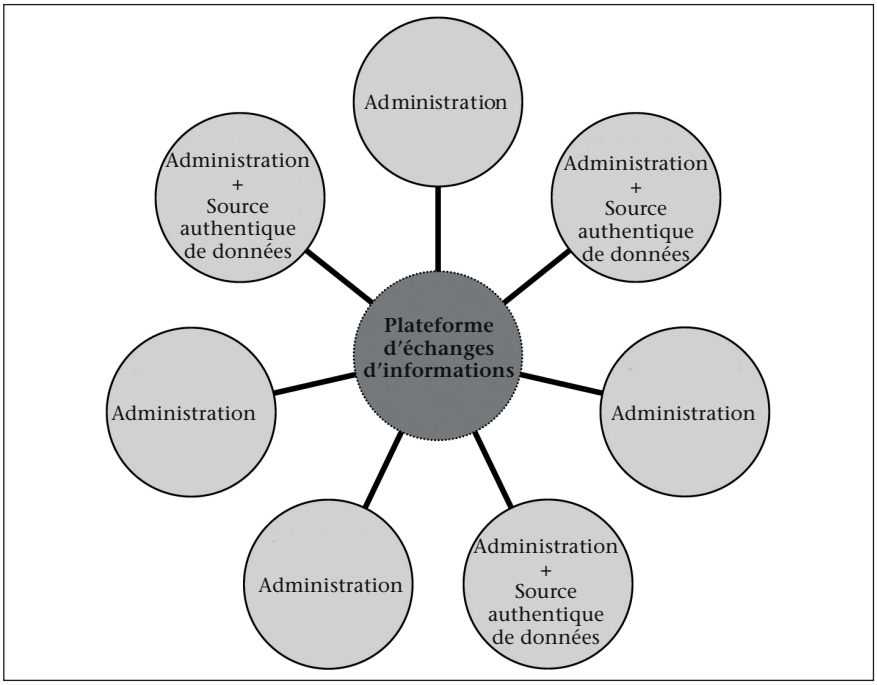

Schéma illustrant un réseau sectoriel composé d'une plateforme d'échanges d'informations à laquelle sont reliées plusieurs administrations dont certaines détiennent une source authentique de données.

A. La source authentique de données

13.- Considérations générales. Dans l'e-gouvernement, les données des citoyens sont enregistrées dans des sources authentiques de données qui sont des bases de données d'un type particulier. Après avoir défini cet outil et expliqué sa raison d'être, l'exemple du Registre national illustrera nos propos.

§1. Définition et raison d'être

14.- Définition. La source authentique de données ne fait pas l'objet d'une définition uniforme. Les caractéristiques de cet outil important de l'e-gouvernement se trouvent dans des textes épars[32]. On constate que

[32] E. Degrave, « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée », *C.D.P.K.*, 2007, p. 51.

certaines normes législatives la définissent explicitement[33]. D'autres normes n'usent pas de ce terme mais organisent en réalité un tel outil[34]. Par ailleurs, il est fait allusion à la source authentique de données dans différents textes tels que des accords de coopération, des rapports parlementaires, des notes stratégiques et certains avis de la CPVP[35].

---

[33] Art. 2, 2°, du décret flamand du 18 juillet 2008 relatif à l'échange électronique de données administratives, *M.B.,* 29 octobre 2008 ; art. 2, 1°, du décret flamand du 13 juillet 2012 portant création et organisation d'un intégrateur de services flamand, *M.B.,* 1er août 2012 ; art. 2, 6°, de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, *M.B.,* 29 août 2012 (ci-après « loi du 15 août 2012 sur l'intégrateur de services fédéral) ; art. 2, 1°, de l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.,* 23 juillet 2013.

[34] Loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.,* 21 avril 1984, ci-après « loi sur le Registre national » (comme l'affirme la CPVP, « la loi n'utilise pas le terme 'source authentique' mais tout indique que le Registre national en est une » [voy. la recommandation n° 09/2012 du 23 mai 2012 relative aux sources authentiques de données dans le secteur public, p. 3, note 7] ; dans le même sens, voy. l'exposé des motifs du projet de loi relatif à la création et à l'organisation d'un intégrateur de services fédéral, *Doc. Parl.,* Ch. Repr., session 2011-2012, n° 53-2223/001, p. 18) ; Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, *M.B.,* 5 février 2003 (contrairement à ce que son nom laisse penser, la Banque-Carrefour des entreprises n'est pas une Banque-Carrefour mais une source authentique de données. En ce sens, voy. Projet de loi relatif à la création et à l'organisation d'un intégrateur de services fédéral, *op. cit.,* p.18) ; Loi du 14 avril 2011 portant des dispositions diverses, en particulier les articles 4 et s. qui organisent la Banque-Carrefour des permis de conduire (comme la Banque-Carrefour des entreprises, la Banque-Carrefour des véhicules est, en partie du moins, une source authentique de données. En ce sens, voy. CPVP, avis n° 14/2010 du 31 mars 2010 sur un avant-projet de loi portant création de la Banque-Carrefour des permis de conduire, p. 3 ; CPVP, avis n° 34/2011 sur un projet d'arrêté royal portant exécution de la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules, p. 5).

[35] Voy. not. le rapport « L'administration électronique au niveau des pouvoirs fédéral, provincial et local », du 16 janvier 2001, *Doc. Parl.,* Sénat, sess. ord. 2000-2001, n° 2-564/1, p. 10 ; art. 7 de l'accord de coopération du 23 mars 2001 entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire flamande, la Commission communautaire française et la Commission communautaire commune concernant la construction et l'exploitation d'une e-plate-forme commune, *M.B.,* 8 août 2001 ; Note stratégique 2003 du Secrétaire d'État à l'Informatisation de l'État, p. 8 ; Accord de coopération du 19 octobre 2006 entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire française et la Commission communautaire commune concernant les principes pour un e-gouvernement intégré et la construction, l'utilisation et la gestion de développements et de services d'un e-gouvernement intégré, *M.B.,* 19 octobre 2006 ainsi que la résolution sur l'*e-government* intégré en exécution de

À partir des divers éléments mentionnés dans ces textes, une définition de cette notion peut être proposée. Ainsi, une « source authentique de données » est une base de données désignée comme telle par une norme de valeur législative[36], contenant des informations relatives à des personnes physiques ou morales, qui ont une valeur unique dans l'administration car leur collecte, leur enregistrement, leur mise à jour et leur destruction sont assurés exclusivement sous la responsabilité d'une administration déterminée, appelée « administration détentrice », et qui sont destinées à être réutilisées par les administrations.

Il existe déjà plusieurs sources authentiques dans l'administration, chacune regroupant des données relatives à certaines problématiques juridiques.

> Par exemple, le Registre national est une source authentique où sont enregistrées les données relatives à l'identification des personnes, le registre de la DIV est la source authentique des données relatives à l'immatriculation des véhicules, la Banque-Carrefour des entreprises est la source authentique des données relatives à l'identification des entreprises, etc.

15.- Raison d'être. La raison d'être de la source authentique de données est la mise en œuvre du principe de la collecte unique des données. Comme l'a souligné l'introduction de ce chapitre[37], le principe de la collecte unique est de ne collecter qu'une seule fois l'information auprès du citoyen. Pour ne pas bloquer les administrations lorsqu'elles ont besoin des données qu'elles n'ont pas collecté elles-mêmes, le principe de la collecte unique suppose que soit organisée, en parallèle, la réutilisation

---

cet accord de coopération disponible sur le site http://www.fedict.belgium.be/fr/binaries/Resolution_eGov_Congress_Final_FR_tcm166-16731.pdf ; CPVP, avis n° 14/2005 du 28 septembre 2005 faisant suite à une décision d'évocation dans les dossiers SCSZ/05/70, SCSZ/05/90, SCS/05/110 et SCSZ/05/113 transmise par le Président du Comité sectoriel de la Sécurité sociale, p. 3 ; CPVP, avis n° 42/2006 du 18 octobre 2006, concernant l'avant-projet de loi portant création d'une source authentique des données relatives aux véhicules, pp. 3, 6 et 8 ; CPVP, avis n° 11/2007 du 21 mars 2007 relatif à un avant-projet de loi réglant l'application automatique des prix maximaux pour la fourniture d'électricité et de gaz naturel aux clients protégés résidentiels à revenus modestes ou à situation précaire, p. 3 ; CPVP, avis n° 30/2007 du 17 octobre 2007 concernant le projet d'arrêté royal visant à améliorer la mise à jour de l'information relative à la profession au Registre national des personnes physiques, p. 4 ; CPVP, avis n° 23/2008 du 11 juin 2008 relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules.

[36] Il revient au législateur de désigner les sources authentiques de données existant dans l'administration. Cette précision est développée dans le Titre I consacré à la légalité de l'e-gouvernement. Voy. *infra*, n° 103.-

[37] Voy. *supra,* n° 10.-

des informations entre les administrations. On comprend alors que les informations réutilisées doivent être fiables, c'est-à-dire correctes et à jour. Si tel n'est pas le cas, l'erreur affectant l'information réutilisée sera démultipliée autant de fois qu'il y a eu de réutilisations de la donnée erronée.

Ce souci d'unicité de la collecte et de réutilisation de données fiables explique la création de l'outil qu'est la source authentique de données. Le système est conçu comme suit : une fois l'information collectée, elle est enregistrée à un seul endroit, la source authentique de données. Celle-ci est placée sous la responsabilité d'une administration, appelée « administration détentrice »[38]. C'est à cette dernière, exclusivement, que revient l'obligation d'assurer la fiabilité des données de la source authentique de données, de manière à ce que d'autres administrations puissent les réutiliser en toute confiance[39].

§2. L'exemple du Registre national

16.- Une source authentique de données. Le Registre national des personnes physiques, régi par la loi du 8 août 1983 organisant un registre national des personnes physiques[40], est une source authentique de données[41]. Il répond aux caractéristiques de cette notion, comme on l'explique ci-après en soulignant le caractère unique et fiable des données enregistrées au Registre national.

17.- Des données uniques. Le Registre national est une banque de données contenant les données d'identification des citoyens.

Les treize informations d'identification enregistrées au Registre national sont reprises à l'article 3 de la loi sur le Registre national. Il s'agit notamment des nom et prénoms, de l'adresse, de l'état civil, du sexe[42], concernant toutes les personnes physiques inscrites dans certains registres

---

[38] La question de la détermination de l'administration responsable de chaque source authentique sera étudiée *infra,* n°s 193.- et s.

[39] Pour un exemple de réutilisation des données des sources authentiques, voy. *infra,* n° 44.- à propos de l'entrepôt de données.

[40] Ci-après, « loi sur le Registre national ».

[41] CPVP, avis n° 14/2005 du 28 septembre 2005, *op. cit.,* p. 3 ; CPVP, recommandation n° 09/2012, *op. cit.,* p. 3, note 7] ; Projet de loi relatif à la création et à l'organisation d'un intégrateur de services fédéral, Exposé des motifs, précité, p. 18 ; Note stratégique 2003 du Secrétaire d'État à l'Informatisation de l'État, *op. cit.,* p. 8.

[42] L'article 3 de la loi du 8 août 1983 sur le Registre national prévoit l'enregistrement de treize données au Registre national, auxquelles s'ajoute une quatorzième donnée pour les étrangers inscrits au registre d'attente. Il faut préciser que l'historique de ces informations est également enregistré au Registre national, ainsi que les « types d'information » prévus

« papiers » disséminés dans tout le pays, à savoir, les registres de la population et les registres des étrangers tenus dans les communes[43], les registres tenus dans les missions diplomatiques et les postes consulaires belges à l'étranger[44], et les registres d'attente tenus par les communes où sont inscrits les étrangers qui se déclarent réfugiés ou qui demandent la reconnaissance de la qualité de réfugié[45].

Ces informations ont une valeur unique dans l'administration, ce qui signifie qu'en principe[46], elles ne sont enregistrées qu'au Registre national. Dès lors, l'institution qui a besoin d'une donnée d'identification d'un citoyen doit, pour l'obtenir, s'adresser au Registre national et non plus au citoyen.

Ainsi, comme l'affirme la loi sur le Registre national depuis une modification intervenue en 2003[47], « les autorités, les organismes et les personnes […] qui sont autorisés [par la loi] à consulter le Registre national ne peuvent plus demander directement lesdites données à une personne »[48]. Par conséquent, « dès qu'une donnée a été communiquée au Registre national et enregistrée dans ledit registre, la personne concernée n'est pas tenue de la communiquer directement aux autorités,

par l'arrêté royal du 8 janvier 2006 déterminant les types d'information associés aux informations visées à l'article 3, alinéa 1er, de la loi du 8 août 1983 sur le Registre national. Nous y reviendrons plus loin. Voy. *infra,* n° 111.-

[43] Le registre de la population contient les données relatives aux Belges, tandis que le registre des étrangers contient les données relatives aux étrangers admis ou autorisés à s'établir ou à séjourner dans le Royaume [Projet de loi créant un registre d'attente pour les étrangers qui se déclarent réfugiés ou qui demandent la reconnaissance de la qualité de réfugié. Rapport fait au nom de la Commission de l'intérieur par M. Cannaerts, *Doc. parl,* Sénat, sess. ord. 1993-1994, n° 1015-2, p. 2]. Ces deux types de registres sont généralement regroupés sous le vocable générique de registres de la population, comme le prévoit l'article 1 de la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité.

[44] Même si la loi ne le précise pas, dans ce cas, seuls les ressortissants belges sont enregistrés au Registre national [Rapport au Roi précédant l'arrêté royal du 3 avril 1984 relatif à l'accès de certaines autorités publiques au Registre national des personnes physiques, ainsi qu'à la tenue à jour et au contrôle des informations, *M.B.,* 21 avril 1984, également publié dans *Pasin.,* 1984, p. 687].

[45] Art. 2, al. 1er, de la loi sur le Registre national.

[46] Nous nuançons notre propos dans la mesure où, pour l'heure, de nombreux duplicata des données d'identification des citoyens existent dans les administrations. Cela tient au fait que la mise en œuvre du principe de la collecte unique des données est relativement récente, ce qui devrait changer à l'avenir.

[47] Art. 5 de la loi du 25 mars 2003 modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.,* 25 mars 2003.

[48] Art. 6, §1, de la loi sur le Registre national.

organismes et personnes […] qui sont autorisés [par la loi] à consulter les données du Registre national »[49].

De cette manière, le Registre national rend possible la collecte unique des données d'identification et épargne aux citoyens un certain nombre de démarches administratives.

> Prenons l'exemple de deux personnes qui se marient. Avant la modification de la loi en 2003, elles devaient fournir à la commune où elles allaient se marier la preuve de leur nationalité, de leur célibat et de leur inscription dans le registre de la population ou dans le registre des étrangers et ce, en vue de permettre la déclaration de mariage.
>
> Depuis cette modification de 2003 et la consécration légale du principe de la collecte unique des données, l'Officier de l'état civil, qui est autorisé par la loi à accéder au Registre national, doit lui-même produire ces preuves, soit en les demandant aux communes concernées, soit en accédant au Registre national.

De plus, depuis une modification législative intervenue le 25 avril 2007[50], la loi sur le Registre national consacre la force probante des informations enregistrées au Registre national, en affirmant que les informations du Registre national « font foi jusqu'à preuve du contraire » et « peuvent être valablement utilisées en remplacement des informations contenues dans les registres [détenus par les communes, les missions diplomatiques et les postes consulaires] ».

Compte tenu du fait que les informations centralisées au Registre national ont la même force probante que ces mêmes informations disséminées dans les registres détenus par les communes, les missions diplomatiques et les postes consulaires, on peut raisonnablement penser qu'il est plus aisé de trouver les informations au Registre national que dans les différents registres susmentionnés. En d'autres termes, les autorités disposant de l'accès au Registre national sont incitées à faire usage de cet accès au Registre national plutôt que de s'adresser aux communes, missions diplomatiques et postes consulaires. Dans le même temps, l'accès aux données du Registre national facilite les démarches des citoyens qui peuvent rapidement obtenir les extraits du Registre national qui leur sont réclamés en se connectant au Registre national depuis leur ordinateur.

> Pour reprendre l'exemple de l'Officier de l'État civil chargé de récolter les preuves nécessaires à une déclaration de mariage, il est encouragé à le faire via le Registre national puisque, depuis 2007, la force probante des extraits du Registre national est certaine.

---

[49] *Idem*.

[50] Art. 4 de la loi du 25 avril 2007 portant des dispositions diverses, *M.B.*, 8 mai 2007.

Par ailleurs, les tâches administratives de chaque citoyen sont facilitées. Par exemple, lorsqu'il doit fournir un extrait du registre national, tel qu'un certificat de nationalité, à une autorité qui n'a pas accès à la source authentique, l'individu ne doit pas se déplacer jusqu'à sa commune. Il peut obtenir cet extrait grâce au site internet https://mondossier.rrn.fgov.be, en utilisant sa carte d'identité électronique et un lecteur de carte. Cet extrait est généré en format PDF et a une force probante équivalente aux extraits des registres de la population, qu'il soit transmis à l'autorité demanderesse sous forme papier ou sous forme électronique.

18.- Des données fiables. Le SPF Intérieur est responsable du Registre national et de la fiabilité des données enregistrées dans cette source authentique[51].

En pratique, à la différence d'autres administrations détentrices de sources authentiques, le SPF Intérieur n'assure pas lui-même la collecte et la mise à jour des données enregistrées au Registre national. Cette tâche incombe aux communes, aux missions diplomatiques et aux postes consulaires qui doivent au préalable vérifier que les informations qu'ils transmettent au Registre national sont conformes aux registres papiers détenus par eux, comme les y oblige la loi[52]. La mise à jour des données du Registre national incombe également à ces autorités, puisque la loi leur impose de communiquer les modifications successives de ces données ainsi que leur date de prise d'effet[53]. Cette particularité semble liée au fait que le Registre national contient des données issues de registres « papiers » détenus par les communes, les missions diplomatiques et les postes consulaires.

Même si le SPF Intérieur n'assure pas lui-même la collecte et la mise à jour des données du Registre national, il n'en demeure pas moins responsable de la source authentique dont il est l'administration détentrice. En d'autres termes, si un préjudice est causé suite à l'utilisation de données fausses issues du Registre national, la responsabilité du SPF Intérieur pourra être engagée. C'est la raison pour laquelle le SPF Intérieur veille au bon accomplissement des tâches en la matière, ce qu'il fait, par exemple, en adressant aux autorités concernées des circulaires relatives la transmission des informations au Registre national[54].

---

[51] CPVP, avis n° 14/2005 du 28 septembre 2005, *op. cit.,* p. 3.

[52] Art. 3 de la loi sur le Registre national.

[53] Art. 3 et 4 de la loi sur le Registre national.

[54] Voy. *infra* n° 406.- Voy., not., la circulaire du 1er août 2005 relative à la tenue à jour des registres de la population et du Registre national des personnes physiques, et, plus particulièrement, aux retards éventuels dans les mises à jour de certaines informations importantes, disponible sur le site du Registre national (http://www.ibz.rrn.fgov.be) Le SPF Intérieur y rappelle notamment « la responsabilité qui incombe à l'administration communale quant à l'exactitude des informations qui sont communiquées aux intéressés mêmes, ainsi qu'à

B. La plateforme d'échanges d'informations

19.- Considérations générales. Comme on l'a dit, le principe de la collecte unique des données va de pair avec la réutilisation des données au sein de l'administration. C'est à cette fin qu'a été créée la plateforme d'échanges d'information.

Après avoir défini cet outil et expliqué sa raison d'être, la Banque-Carrefour de la sécurité sociale est analysée en guise d'exemple de plateforme d'échanges d'informations.

§1. Définition et raison d'être

20.- Définition. Tout comme la source authentique de données, la notion de « plateforme d'échanges d'informations » ne fait pas l'objet d'une définition uniforme.

Toutefois, à partir de différents textes qui se réfèrent à cette notion[55], on peut définir la plateforme d'échanges d'informations comme « une infrastructure technique constituant le noyau central d'un réseau sectoriel, et qui a pour fonction d'organiser l'échange électronique de données au sein de ce réseau sectoriel ».

Il y a lieu de remarquer que la plateforme d'échanges d'informations est parfois appelée « Banque-Carrefour »[56]. Nous choisissons de ne pas

---

des tiers qui ont accès à ces informations, notamment via le Registre national des personnes physiques ». Le SPF Intérieur y rappelle le délai dans le lequel les informations enregistrées dans les registres communaux doivent parvenir au Registre national. Par exemple, en vertu de l'art. 6, §3, de l'arrêté royal du 3 avril 1984 relatif à l'accès de certaines autorités publiques au Registre national des personnes physiques, ainsi qu'à la tenue à jour et au contrôle des informations précité, le service de la population dispose de deux jours ouvrables, après avoir établi l'acte de naissance (ce qui doit se faire, selon le SPF, en deux ou trois jours ouvrables après la déclaration de naissance), pour introduire les informations au Registre national. Le SPF Intérieur énonce également une procédure permettant de détecter et de résoudre « les retards excessifs ou répétés » en ce domaine.

[55] Voy. not. la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.,* 22 février 1990 (ci-après « loi sur la Banque-Carrefour de la sécurité sociale ») ainsi que les travaux préparatoire de celle-ci (*Pasin.* 1990, I, pp. 58-146, spéc. 77-80) ; loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules, *M.B.,* 28 juin 2010 (ci-après « loi sur la Banque-Carrefour des véhicules ») ; CPVP, avis n° 14/2005 du 28 septembre 2005 faisant suite à une décision d'évocation dans les dossiers SCSZ/05/70, SCSZ/05/110 et SCSZ/05/113 transmise par le Président du Comité sectoriel de la Sécurité sociale, pp. 7 et 8 ; CPVP, avis n° 14/2008 du 2 avril 2008 concernant un projet de loi portant institution et organisation de la plateforme eHealth (A/2008/016), pp. 10, 21, 22 ; CPVP, avis n° 42/2006, *op. cit.,* p. 13.

[56] Voy. la loi sur la Banque-Carrefour de la sécurité sociale et la loi sur la Banque-Carrefour des véhicules.

utiliser ce terme car le terme « banque » peut induire en erreur en laissant à penser qu'il s'agit d'une base de données contenant des données à caractère personnel des citoyens, ce qui n'est pas le cas, en principe.

Le terme « intégrateur de services » est également utilisé pour désigner ce type d'outil[57]. Nous préférons ne pas l'utiliser non plus car il est d'emblée peu parlant et que la définition qu'en donne la CPVP semble conférer à cet outil une portée plus vaste que celle d'une plateforme d'échanges d'informations dans le sens où nous l'entendons ici[58].

> Par exemple, la Banque-Carrefour de la sécurité sociale, pour la sécurité sociale[59], la plateforme *eHealth*[60], dans le domaine de la santé, et l'intégrateur de services fédéral[61], qui organise la collaboration électronique entre autorités fédérales, répondent aux caractéristiques de la plateforme d'échanges d'informations.
>
> Par contre, la Banque-Carrefour des entreprises ne répond que très partiellement à la définition de cette notion, contrairement à ce que son nom semble indiquer. Elle présente des caractéristiques de la source authentique de données et de la plateforme d'échanges d'informations. Néanmoins, elle s'apparente davantage à la première qu'à la seconde[62]. Il en va de même de

[57] Voy. not. la loi du 15 août 2012 précitée, relative à la création et à l'organisation d'un intégrateur de services fédéral.

[58] En effet, sans sa recommandation n° 03/2009 précitée, la CPVP définit l'intégration de services comme « l'harmonisation de services électroniques partiels en un ensemble cohérent de services électroniques en vue de le proposer à des tiers ».

[59] Loi sur la Banque-Carrefour de la sécurité sociale, précitée.

[60] Loi du 21 août 2008 relative à l'institution et à l'organisation de la plateforme *eHealth, M.B.,* 13 octobre 2008.

[61] Loi sur l'intégrateur de services fédéral, précitée.

[62] La Banque-Carrefour des entreprises (ci-après « BCE ») est organisée par la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, *M.B.,* 5 février 2003. La BCE s'apparente à la source authentique de données sous deux aspects principalement. D'une part, il s'agit d'une banque de données (l'article 3 de la loi la définit comme un « registre ») détenue par le SPF Économie, P.M.E., Classes moyennes et Énergie. Il ne s'agit donc pas d'une infrastructure technique. D'autre part, cette base de données contient des données de contenu –telles que les données d'identification des fondateurs de chaque société, par exemple- et non seulement la référence à des données détenues au sein des administrations qui seraient reliées à la BCE. Par conséquent, la BCE ne gère pas un répertoire de références. En outre, les administrations consultent les données qui sont stockées à la BCE et ne se contentent pas de réclamer des données qui devraient ensuite leur être acheminées depuis une autre institution via la plateforme. Néanmoins, comme une plateforme d'échanges d'informations, cette base de données est assortie d'une « fonction 'carrefour' qui lui permet d'informer les diverses autorités publiques à tout moment des données d'identification les plus récentes ainsi que de toutes les modifications apportées aux renseignements qui les concernent ». [Projet de loi portant création d'une BCE […], *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50 2058/00, p. 7]. En outre, l'enregistrement

la Banque-Carrefour des véhicules[63] et de la Banque-Carrefour des permis de conduire[64].

21.- Raison d'être. La raison d'être de la plateforme d'échanges d'informations est la circulation des informations entre les administrations, dans le but de rendre plus efficace l'exécution des tâches administratives, et de protéger la vie privée des citoyens.

Grâce à la plateforme d'échanges d'informations, les *tâches administratives sont allégées*. L'autorité publique ne doit plus elle-même collecter, auprès du citoyen, l'ensemble des données dont elle a besoin, ni veiller à leur mise à jour. Si l'autorité ne dispose pas de l'information nécessaire, il lui suffit de la demander à la plateforme d'échanges d'informations qui la lui fournira. Outre le gain de temps que cela représente, nombre d'erreurs administratives sont ainsi évitées puisqu'on n'encode pas la même information à de multiples reprises.

Par ailleurs, la plateforme d'échanges d'information favorise la *protection de la vie privée* des citoyens. Elle permet d'éviter la centralisation des données au sein d'une grande base de données détenue par l'État. Une telle centralisation constituerait un danger important pour la protection de la vie privée des citoyens puisqu'il suffirait d'accéder à cette base de données pour connaître toutes les informations de tous les citoyens[65]. Grâce à la plateforme d'échanges d'informations, les informations sont rendues disponibles au sein de l'administration, bien qu'elles soient enregistrées dans des bases de données différentes – les sources authentiques de données –, disséminées au sein d'institutions diverses pour éviter la constitution d'une énorme base de donnée centralisée.

---

des données contenues dans la BCE se fonde sur une répartition fonctionnelle entre les autorités, les administrations et les services qui sont chargés de la collecte unique de ces données et de leur mise à jour. Cette répartition n'est toutefois pas effectuée par la BCE mais par le Roi (art. 7 de la loi). [Sur les différences énoncées, voy. le projet de loi portant création d'une BCE […], *op. cit.,* pp. 5-7, 19, 26, 94, 101, 102 ; avis CPVP n° 07/2002 du 11 février 2002 relatif au projet de loi créant une Banque-Carrefour des entreprises, pp. 4, 5 et 8 ; D. Van Kriekinge, « La Banque-Carrefour des Entreprises en tant que pilier de réalisation de l'*e*-gouvernement : un pas vers la simplification administrative ? », *R.D.T.I.,* 2004, p. 8 ; D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank vanOndernemingen en de elecktronische identiteitskaart als belangrijkste juridische bouwstenen,* Brugge, Vandenbroele, 2005, p. 86, n° 204].

[63] Voy. not. CPVP, avis n° 34/2011, *op. cit.*, p. 5.

[64] Voy. not. CPVP, avis n° 14/2010, *op. cit.*, p. 3.

[65] Voy. not. S. Gutwirth, *Waarheidsaanspraken in Rechten wetenschap,* Bruxelles, Maklu, 1993, pp. 667 et s. ; H. Maisl, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », *in L'administration électronique au service des citoyens* (dir. G. Chatillon et B. du Marais), Bruxelles, Bruylant, 2003, pp. 349 à 351. Voy. égal. *infra,* n°s 59 et s.

Les discussions parlementaires qui ont précédé l'adoption de la loi sur la Banque-Carrefour de la sécurité sociale[66] témoignent du souci de protéger la vie privée des citoyens en ne créant pas une base de données centralisée. En effet, originairement, un premier projet de loi datant de 1981 envisageait la Banque-Carrefour comme une banque de données « mammouth »[67] contenant l'enregistrement de toutes les données à caractère personnel relatives à la sécurité sociale. Des voix se sont élevées contre la mise en place d'un tel outil, au motif qu'il constituait une menace pour la vie privée des citoyens[68]. Pour endiguer ces craintes, il a été décidé d'organiser un enregistrement décentralisé et unique des données au sein du réseau sectoriel de la sécurité sociale. Dans ce cadre, la Banque-Carrefour ne joue que le rôle d'une plaque tournante d'informations, qui coordonne les échanges d'informations entre ces organismes de sécurité sociale. De cette manière, on respecte les compétences de chaque organisme tout en assurant une collaboration ordonnée entre eux[69].

Les craintes liées à la centralisation des données étaient déjà apparues en dehors des frontières belges, en France notamment. Quelques années avant les premières discussions relatives à la Banque-Carrefour de la sécurité sociale, un projet de centralisation de données dénommé SAFARI avait été envisagé pour l'administration française. Il avait suscité tant d'émoi qu'il avait été abandonné. Dans le même temps, on a adopté la Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pour encadrer les traitements de données en France et instituer une autorité nationale de protection des données. Nous y reviendrons[70].

---

[66] Cette plateforme d'échanges de données est étudiée ci-après, voy. n°s 23.- et s.

[67] J. Viaene, « Le plan d'informatisation de la sécurité sociale », *Rev. b. séc. soc.,* 1989, numéro spécial, p. 14.

[68] F. Robben, « Le projet de loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale », *op. cit.,* p. 74 ; F. Ringelheim, « Vie privée et protection des données sociales », *op. cit.,* p. 302 ; F. Ringelheim, « La protection des banques de données et la sécurité sociale », *op. cit.*, p. 94.

[69] Projet de loi relatif à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *Doc. Parl.,* Ch. Repr., sess. 1988-1989, n° 899/1, *Pasin,* 1990, I, pp. 77-78 ; Rapport fait au nom de la Commission des affaires sociales par Mme Nelis- Van Liedekerke, *Doc. Parl.,* Ch. Repr., 1988-1989, n° 899/4, publié dans *Pasin.,* 1990, I, p. 110 ; F. Ringelheim, « La protection des banques de données et la sécurité sociale », *op. cit.*, p. 94 ; J. Viaene, *op. cit.,* p. 15 ; F. Ringelheim, « Vie privée et protection des données sociales », *op. cit.,* p. 303 ; F. Robben, « Le fonctionnement de la Banque-Carrefour de la sécurité sociale », *op. cit.,* p. 55.

[70] Voy. *infra,* n° 63.-

§2. L'exemple de la Banque-Carrefour de la sécurité sociale

22.- Une plateforme d'échanges d'informations. La Banque-Carrefour de la sécurité sociale[71] est une plateforme d'échanges d'informations. Elle est en effet une infrastructure technique, placée au cœur d'un réseau sectoriel, et organisant l'échanges de données entre les administrations de ce réseau.

23.- Une infrastructure technique. La Banque-Carrefour est une infrastructure technique, qui exécute certaines tâches, grâce à des outils informatiques, du personnel, un patrimoine, etc.

Cette infrastructure a été constituée par la loi sous la forme d'un établissement public[72], au sein du SPF Sécurité sociale[73]. La loi sur la Banque-Carrefour de la sécurité sociale confère à cette institution la personnalité juridique[74]. Elle lui octroie également des droits et lui impose des obligations, organisant ainsi une décentralisation par services.

La Banque-Carrefour bénéficie de certains droits. En effet, elle jouit d'une autonomie technique, puisqu'elle gère un patrimoine que la collectivité fédérale, recourant au mécanisme de la fondation, lui a affecté, en vue de satisfaire des intérêts publics en matière de sécurité sociale. Elle bénéficie notamment d'une dotation annuelle en provenance du SPF Sécurité sociale, ainsi que d'une participation des institutions de sécurité sociale[75]. La Banque-Carrefour jouit également d'une autonomie organique. Elle peut prendre des décisions par l'intermédiaire de son comité de gestion[76]. Le Ministre dirigeant le SPF sécurité sociale ne fait partie de cet organe de décision. Il ne peut donc exercer sur celui-ci un contrôle hiérarchique en lui imposant des injonctions ou des instructions à suivre.

La Banque-Carrefour est également soumise à certaines obligations. Elle doit exercer ses compétences conformément à un contrat d'administration

---

[71] Ci-après, « la Banque-Carrefour ».

[72] Un établissement public peut être défini comme un type d'organisme public personnalisé et décentralisé, « constitué par le procédé de la fondation, jouissant d'une autonomie organique et technique, et doté d'organes de gestion parmi lesquels ne figure pas le ministre qui dirige le SPF ou le ministère dont dépend l'établissement ». [Y. LEJEUNE, « Chapitre 1er. L'organisation des pouvoirs publics », *DIMM,* fasc. 53, Bruxelles, Story-Scientia, 2007, p. 41].

[73] Art. 1 de la loi sur la Banque-Carrefour de la sécurité sociale.

[74] *Ibid.,* art. 1.

[75] *Ibid.,* art. 35.

[76] *Ibid.,* art. 31.

qui la lie à l'État fédéral et sous le contrôle d'une autorité de tutelle[77], conformément à un arrêté royal du 3 avril 1997[78]. Elle doit donc respecter le principe de spécialité des autorités administratives et agir dans le respect de la Constitution et des lois qui lui sont applicables. En l'espèce, il s'agit principalement de la loi sur la Banque-Carrefour de la sécurité sociale et de la loi du 8 décembre 1992 sur la protection de la vie privée.

24.- Le noyau d'un réseau sectoriel. La Banque-Carrefour constitue le noyau du réseau sectoriel de la sécurité sociale.

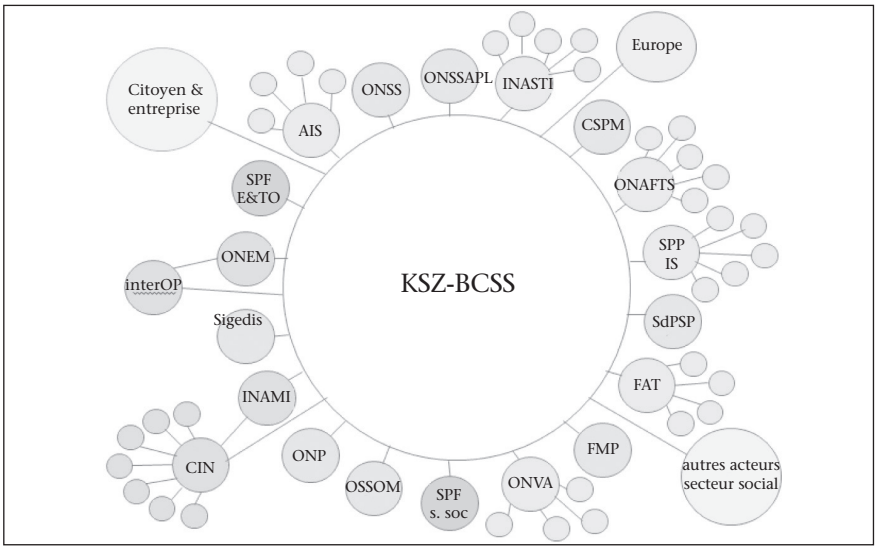

Schéma illustrant le réseau sectoriel de la sécurité sociale comprenant, en son cœur, la Banque-Carrefour de la sécurité sociale[79].
« KSZ-BCSS » est l'acronyme de « Kruispuntbank van de Sociale Zekerheid – Banque-Carrefour de la sécurité sociale ».

[77] Cette autorité de tutelle est déterminée, en début de législature, par une décision du Conseil des ministres, généralement confirmée par arrêté royal. Actuellement, la tutelle sur la Banque-Carrefour est exercée conjointement par la ministre de l'Emploi et la ministre des affaires sociales [Art. 19 de l'arrêté royal du 17 avril 2008 fixant certaines attributions ministérielles, *M.B.*, 24 avril 2008].

[78] Arrêté royal du 3 avril 1997 portant des mesures en vue de la responsabilisation des institutions publiques de sécurité sociale, en application de l'art. 47 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux de pensions, *M.B.*, 30 avril 1997.

[79] Ce schéma est disponible sur le site de la Banque-Carrefour de la sécurité sociale, à l'adresse www.ksz-bcss.fgov.be/fr/bcss/page/content/websites/belgium/about/mission/structure.html

Comme le montre ce schéma, outre la plateforme d'échanges d'informations qu'est la Banque-Carrefour, le réseau sectoriel de la sécurité sociale comprend également les institutions de sécurité sociale, ainsi que le Registre national et le SPF Technologie de l'Information et de la Communication, dit « SPF Fedict »[80]. Entre ces autorités s'organise l'échange d'informations issues de différentes sources authentiques, comme l'expliquent les lignes qui suivent.

a) Les autorités appartenant au réseau sectoriel de la sécurité sociale. Le réseau sectoriel de la sécurité sociale comprend, tout d'abord et principalement, les institutions de sécurité sociale entendues au sens large du terme[81]. Parmi celles-ci, certaines appartiennent au réseau primaire tandis que d'autres sont regroupées au sein d'un réseau secondaire.

Le réseau primaire est constitué de la Banque-Carrefour, entourée d'un premier cercle d'institutions de sécurité sociale, à savoir, les organismes publics de sécurité sociale[82]. Ces derniers sont directement reliés à la Banque-Carrefour et placés sous la tutelle du Ministre des Affaires sociales ou du Ministre de l'Emploi.

---

[80] L'art. 2, de la loi sur la Banque-Carrefour de la sécurité sociale définit le réseau de la sécurité sociale comme « l'ensemble constitué par les banques de données sociales, la Banque-Carrefour et le Registre national [...] », et les banques de données sociales comme « les banques de données où des données sociales sont conservées par les institutions de sécurité sociale ou pour leur compte ». Pourtant, la loi prête parfois à confusion lorsqu'elle laisse à penser que ce sont les institutions de sécurité sociale dans leur ensemble, et non seulement leur base de données sociale, qui fait partie du réseau (voy. par exemple, l'art. 18 de la loi, qui prévoit que le réseau peut être étendu « à d'autres personnes que les institutions de sécurités sociale » et que « ces personnes sont intégrées dans le réseau dans la mesure de l'extension décidée »). À notre sens, la question de savoir si le réseau de la sécurité sociale comprend seulement les bases de données sociales ou également les institutions de sécurité sociale importe peu. Pour plus de clarté, nous considérons que ce réseau sectoriel comprend la Banque-Carrefour, les institutions de sécurité sociale et le Registre national.

[81] Il résulte de l'art. 2, 1°, de la loi sur la Banque-Carrefour de la sécurité sociale, que la notion de sécurité sociale est entendue dans un sens très large, si bien que de nombreuses institutions font partie de ce réseau sectoriel.

[82] Concrètement, il s'agit de l'Association d'institutions sectorielles (AIS), du Comité Individuel Multisectoriel (CIMIRe), du Collège intermutualiste national (CIN), de la Caisse de secours et de prévoyance en faveur des marins (CSP), du Fonds des accidents du travail (FAT), du Fonds des maladies professionnelles (FMP), de l'Institut national d'assurance maladie et invalidité (INAMI), de l'Institut national d'assurance sociales pour travailleurs indépendants (INASTI), de l'Office national d'allocations familiales pour travailleurs salariés (ONAFTS), de l'Office de l'emploi (ONEm), de l'Office national des pensions (ONP), de l'Office national de sécurité sociale (ONSS), de l'Office national des vacances annuelles (ONVA), de l'Office de sécurité sociale d'Outre-mer (OSSOM), du Service des pensions du secteur public (SdPSP), du SPF Emploi, Travail et Concertation sociale (en ce qui concerne les conventions collectives et l'inspection sociale), et du SPF Sécurité sociale.

Un deuxième cercle entoure le premier, et comprend *les réseaux secondaires*. Chaque réseau secondaire correspond à un secteur de la sécurité sociale. Il comprend les organismes de droit privé remplissant des missions de sécurité sociale dans ce secteur, appelés aussi « institutions coopérantes de sécurité sociale » ainsi que leur organisme de tutelle, appelé « institution gérant le réseau secondaire »[83]. Ainsi, par exemple, il existe un réseau secondaire comprenant les caisses d'allocations familiales, l'institution de gestion de ce réseau secondaire et l'Office National des Allocations Familiales pour travailleurs salariés (O.N.A.F.T.S.)[84].

Ces organismes de droit privé ne sont pas directement reliés à la Banque-Carrefour. Ils n'apparaissent donc pas dans son répertoire de références[85]. C'est là tout l'intérêt de la création de ce réseau secondaire. En effet, la mention directe, dans la table de références de la Banque-Carrefour, de l'appartenance à ces organismes de droit privé qui ont souvent été constitués sur une base idéologique ou politique, tels que les syndicats ou les mutuelles, permettrait de divulguer des données considérées comme sensibles car touchant à la liberté d'opinion et donc, à la vie privée des citoyens[86]. Dès lors, le répertoire des références de la Banque-Carrefour ne contient que la mention du réseau secondaire dans lequel la donnée recherchée se situe. L'institution gérant ce réseau secondaire tient, quant à elle, un répertoire sectoriel des références, reprenant, pour chaque donnée

[83] Cette institution appartient au réseau primaire. (Rapport au Roi précédent l'arrêté royal du 4 février 1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale, *M.B.,* 3 avril 1997).

[84] Outre le réseau secondaire dans le secteur des allocations familiales, existent un réseau secondaire dans le secteur des accidents du travail, regroupant les compagnies d'assurance traitant les dossiers en ce domaine, et le Fonds des accidents du travail, *in*stitution de gestion de ce réseau ; un réseau secondaire dans le secteur des vacances annuelles constitué des caisses de vacances et de l'Office national des vacances annuelles, *in*stitution de gestion de ce réseau, et enfin, un réseau secondaire dans le secteur de l'assurance soins de santé et indemnités constitué des organismes assureurs coopérants, de la Caisse auxiliaire d'assurance maladie-invalidité, de la Caisse des soins de santé de la Société nationale des Chemins de fer belges et, enfin, du Collège intermutualiste national qui est l'institution de gestion de ce réseau secondaire. Voy. le Rapport au Roi précédent l'arrêté royal du 4 février 1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale, *M.B.,* 3 avril 1997. Voy aussi J. VIAENE, « Le plan d'informatisation de la sécurité sociale », *Rev. b. séc. Soc.,* 1989, n° spécial, p. 14 ; F. RINGELHEIM, « Vie privée et protection des données sociales », *op. cit.,* p. 305 ; Banque-Carrefour de la sécurité sociale, « Missions. Structure du réseau », disponible sur le site http://www.ksz.fgov.be/fr

[85] Sur cette notion, voy. *infra*, n° 25.-

[86] F. RINGELHEIM, « La protection des banques de données et la sécurité sociale », *Rev. Dr. ULB,* 1994-1995, p. 103 ; F. RINGELHEIM, « Vie privée et protection des données sociales », *Rev. Dr. Soc.,* 1994, p. 305 ; D. PIETERS, « La Banque-Carrefour de la sécurité sociale et la protection de la vie privée », *Rev. B. séc. soc.,* 1989, pp. 55-56.

disponible dans ce réseau secondaire, la mention de l'institution de sécurité sociale de ce réseau où les données sont conservées[87].

D'autre part, le réseau sectoriel de la sécurité sociale comprend une banque de données étrangère à la sécurité sociale, le Registre national, ainsi que le SPF Fedict.

La loi prévoit que le réseau de la sécurité sociale peut être étendu à d'autres institutions, soit en modifiant la notion de « sécurité sociale », de manière à inclure sous le terme « institutions de sécurité sociale », des organismes qui ne sont pas considérés comme tels actuellement, soit en étendant le réseau à d'autres autorités que les institutions de sécurité sociale. Ces deux types d'extension du réseau sectoriel peuvent être effectués par un arrêté royal[88].

b) Les informations circulant au sein du réseau sectoriel de la sécurité sociale. Les institutions de sécurité sociale ainsi que le Registre national s'échangent des informations au sein du réseau sectoriel, par l'intermédiaire de la Banque-Carrefour. Ces informations sont issues du Registre national ou d'une source authentique gérée par une institution de sécurité

[87] Art. 6, al. 2, 2°, de la loi sur la Banque-Carrefour de la sécurité sociale ; art. 1er, 6°, de l'arrêté royal du 4 février 1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale, *M.B.,* 3 avril 1997.

[88] Art. 2, dernier al., de la loi (modification de la notion de « sécurité sociale ») et art. 18 de la loi (extension du réseau à d'autres autorités que les institutions de sécurité sociale). Ainsi, a notamment été adopté l'arrêté royal du 16 janvier 2002 relatif à l'extension du réseau de la sécurité sociale à certains services publics et institutions publiques des Communautés et des Régions, en application de l'art. 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.,* 6 février 2002. Désormais, font partie du réseau sectoriel de la sécurité sociale, les sociétés de logement régionales, les services régionaux de placement (FOREM, VDAB, ORBEM), l'Agence wallonne pour l'intégration des personnes handicapées, etc. D'autres arrêtés royaux relatifs à l'extension du réseau de la sécurité sociale ont été adoptés depuis (Voy. l'arrêté royal du 15 janvier 2004 relatif à l'extension du réseau de la sécurité sociale aux organismes de pension et de solidarité chargés d'exécuter la loi du 28 avril 2003 relative aux pensions complémentaires et au régime fiscal de celles-ci et de certains avantages complémentaires en matière de sécurité sociale, en application de l'art. 18 de la loi du 15 janvier 1990 relative à l'institution d'une Banque-Carrefour de la sécurité sociale, *M.B.,* 14 décembre 2004 ; l'arrêté royal du 15 octobre 2004 relatif à l'extension du réseau de la sécurité sociale aux organismes de pension et de solidarité chargés d'exécuter la loi du 28 avril 2003 relative aux pensions complémentaires et au régime fiscal de celles-ci et de certains avantages complémentaires en matière de sécurité sociale, en application de l'art. 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.,* 14 décembre 2004 ; l'arrêté royal du 4 mars 2005 relatif à l'extension du réseau de la sécurité sociale aux centres publics d'aide sociale, en ce qui concerne leurs missions relatives au droit à l'aide sociale, en application de l'art. 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.,* 31 mars 2005).

sociale. La réponse à la question de savoir quelle information est enregistrée dans quelle source authentique varie suivant le type de source authentique dont émane la donnée.

> Par exemple, le contenu du Registre national est déterminé par la loi du 8 août 1983 sur le Registre national. Toute compétence normative de la Banque-Carrefour relativement au fonctionnement du Registre national est dès lors exclue[89].

Par contre, aucun texte ne définit le contenu des sources authentiques détenues au sein du réseau primaire. Il y a lieu de se référer à la loi sur la Banque-Carrefour qui confie à cette dernière le soin d'effectuer la répartition fonctionnelle des tâches entre les institutions du réseau primaire, après avoir pris l'avis de son Comité général de coordination[90]. Ce faisant, elle détermine quelle instance est chargée « d'enregistrer, de gérer et de mettre à disposition de tous les utilisateurs autorisés quelles informations sous forme authentique »[91], et permet ainsi de définir précisément la responsabilité de chaque institution concernant la collecte et la mise à jour des informations authentiques[92].

En pratique, pour exercer cette répartition, la Banque-Carrefour tient compte de différents critères relatifs, principalement, aux compétences traditionnelles des institutions de sécurité sociale. Ainsi, un document disponible sur le portail de la Banque-Carrefour fait état des « principaux axes de la répartition fonctionnelle »[93] en disposant que :

– « les données d'*identification* sont en premier lieu tenues à jour par le registre national dans lequel sont enregistrées les données de base provenant des registres communaux de population et des étrangers et du registre d'attente [...] ;

---

[89] F. Robben, « Le fonctionnement de la Banque-Carrefour de la sécurité sociale », *Rev. B. séc. Soc.*, 1989, p. 39.

[90] Art. 9 de la loi sur la Banque-Carrefour de la sécurité sociale.

[91] F. Robben et P. Maes, « La Banque-Carrefour de la sécurité sociale comme moteur de l'e-government du secteur social », numéro du 1er juillet 2004, p. 5. Cette compétence de la Banque-Carrefour a été critiquée, au motif qu'il aurait mieux valu confier cette tâche au Comité de surveillance, devenu aujourd'hui le Comité sectoriel, « attendu qu'à cette division de tâche répond la possibilité de recueillir les données correspondantes sans qu'une autorisation du Comité de surveillance soit nécessaire » [D. Pieters, « La Banque-Carrefour de la sécurité sociale et la protection de la vie privée », *Rev. b. séc. soc.*, 1989, p. 63].

[92] Commentaire des articles du projet de loi « relatif à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale », *Doc. Parl.*, 1988-1989, n° 899/1, *Pasin.*, 1990, I, p. 83.

[93] Ce document est disponible sur le site internet de la Banque-Carrefour de la sécurité sociale, dans la rubrique « Missions. Structure du réseau » Voy. http://www.ksz-bcss.fgov.be/fr/bcss/page/content/websites/belgium/about/mission/structure.html

– les données relatives aux *rémunérations* et *au temps de travail* sont recueillies, régulièrement contrôlées et systématiquement tenues à jour par les institutions chargées de la perception des cotisations de sécurité sociale ;
– un aperçu de base par personne des données relatives aux *pensions* et autres avantages en tenant lieu alloués par les institutions débitrices de pensions est géré conjointement par l'Office national des pensions (ONP) et l'Institut national d'assurance maladie et invalidité (INAMI) ;
– l'enregistrement de *la plupart des autres données* est assuré par l'institution qui, dans des conditions normales, utilise le plus ces données ».

25.- L'organisation de l'échange de données grâce à un répertoire de références. La principale mission de la Banque-Carrefour de la sécurité sociale consiste à « conduire, organiser et autoriser les échanges de données sociales entre les banques de données sociales »[94]. La Banque-Carrefour effectue cette tâche grâce à son répertoire des références.

Le répertoire des références est une base de données, détenue et gérée par une plateforme d'échanges d'informations, reprenant uniquement « des références à des informations qui sont tenues de façon décentralisée et distribuée »[95] dans les différentes sources authentiques. Il s'agit, en d'autres termes, d'une « banque de données relationnelle, qui ne garde pas d'information de fond mais uniquement des données 'qui-quoi-où' »[96].

Ainsi, un répertoire de références contient, par citoyen repris dans ce registre sous un numéro d'identification[97], la référence aux sources authentiques dans lesquelles se trouvent des informations à son sujet et le type d'informations dont il s'agit, mais non l'information elle-même. Grâce à cet outil, l'échange d'informations au sein du réseau sectoriel est

[94] Art. 3 de la loi sur la Banque-Carrefour de la sécurité sociale. La Banque-Carrefour exerce également trois autres missions. Ainsi, sa deuxième mission consiste en la coordination entre les institutions de sécurité sociale et le Registre national (art. 1, al. 2, de la loi susvisée). Sa troisième mission consiste en la collecte et l'enregistrement de données d'identification relatives aux personnes qui ne sont pas enregistrées au Registre national (art. 4 de la loi susvisée). Il en sera question dans le chapitre relatif à l'identifiant unique. Sa quatrième et dernière mission consiste en la collecte, auprès des institutions de sécurité sociale, de données sociales pouvant être utiles à la connaissance, à la conception et à la gestion de la sécurité sociale (art. 5 de la loi susvisée).

[95] Banque-Carrefour de la sécurité sociale, « Missions. Structure du réseau », disponible sur le site http://www.ksz.fgov.be/fr

[96] F. Robben, « Le projet de loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale », *D.I.T.,* 1990, p. 76. Dans le même sens, CPVP, avis n° 23/2008, *op. cit.,* p. 6.

[97] Sur cette notion, voy. *infra,* n°s 26.- et s.

rendu possible bien que les informations soient enregistrées de manière décentralisée dans les différentes sources authentiques de ce réseau.

Le répertoire des références de la Banque-Carrefour de la sécurité sociale est structuré en trois tables : la table des autorisations d'accès – appelée également la table « qui-peut obtenir-quoi »[98], la table des données disponibles – appelée également la table « quoi-où »[99] et le répertoire des personnes – appelé également la table « qui-où-quand-en quelle qualité »[100]. De cette manière, une fois saisie d'une demande de données, la Banque-Carrefour peut identifier sa localisation dans le réseau sectoriel, et vérifier si l'administration demanderesse des données est autorisée à y accéder. Ensuite, la Banque-Carrefour procède à l'acheminement de la donnée réclamée.

a) La demande de données. Lorsqu'une institution appartenant au réseau sectoriel de la sécurité sociale a besoin d'une donnée de sécurité sociale qu'elle ne détient pas, elle doit, en principe[101], la demander à la Banque-Carrefour[102]. Il en va de même lorsque la demande d'une donnée de sécurité sociale émane d'une personne ou d'une institution qui n'appartient pas à ce réseau sectoriel[103].

---

[98] Banque-Carrefour de la sécurité sociale, « Flux relatifs au répertoire des références de la Banque-Carrefour », disponible sur le site http://www.ksz.fgov.be/fr

[99] *Idem.*

[100] *Idem.*

[101] La loi sur la Banque-Carrefour de la sécurité sociale prévoit des exceptions à ce principe. Ainsi, l'art. 12 dispose que les institutions de sécurité sociale sont dispensées de passer par la Banque-Carrefour pour les données dont l'enregistrement leur a été confié. Il en va de même lorsqu'elles en ont été dispensées par la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé, dans les cas déterminé par un arrêté royal. En outre, en vertu de l'art. 14, al. 1er, 5° de cette loi, elles ne doivent pas non plus passer par la Banque-Carrefour lorsqu'elles en ont été dispensées par un arrêté royal en vue de remplir leurs missions ou lorsqu'elles savent que les données recherchées se trouvent dans une autre institution de sécurité sociale qui a été autorisée, par arrêté royal, à communiquer des données sans passer par la Banque-Carrefour. Ainsi, l'art. 2 de l'arrêté royal du 4 février 1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale prévoit qu'il ne faut pas passer par la Banque-Carrefour lors d'une communication de données entre institutions d'un réseau secondaire soumise à certaines conditions (art. 2, 2°) ou lors d'une communication de données entre une institution et son sous traitant (art. 2, 1°).

[102] Nous précisions que si l'institution demanderesse appartient à un réseau secondaire, cette demande est adressée à la Banque-Carrefour par l'intermédiaire de l'institution gérant ce réseau secondaire.

[103] Dans cette hypothèse, le demandeur de la donnée est dispensé d'adresser sa demande à la Banque-Carrefour dans les cas prévus à l'art. 14 de la loi sur la Banque-Carrefour de la sécurité sociale. Cette disposition prévoit des exceptions au principe du passage par la Banque-Carrefour, liées soit à la qualité de la personne demanderesse (1° à 4°) soit à l'institution détentrice de la donnée (5°). Ainsi, ne doivent pas demander l'intervention de la Banque-Carrefour, et peuvent donc obtenir les informations directement de l'institution

> Par exemple, l'ONEm et les organismes de paiement des allocations de chômage ont besoin, pour établir le passé professionnel du chômeur, de connaître notamment les années de carrière et nombre de jours de travail prestés durant ces années. Puisqu'elles ne détiennent pas ces informations, elles demandent à la Banque-Carrefour de les trouver et de les leur acheminer ensuite.

b) La vérification effectuée par la Banque-Carrefour. Une fois saisie de la demande d'une donnée, la Banque-Carrefour vérifie d'abord si l'institution demanderesse est *autorisée* à l'obtenir. La Banque-Carrefour n'autorise pas elle-même l'accès aux données détenues par les institutions de sécurité sociale. Cette tâche relève de la compétence du Comité sectoriel de la santé et de la sécurité sociale[104]. Il revient seulement à la Banque-Carrefour de vérifier que l'institution a bien été autorisée par le Comité sectoriel à accéder à la donnée qu'elle réclame. Cette vérification est effectuée à partir de la table des autorisations d'accès, qui reprend, pour chaque institution, les données pour lesquelles celle-ci a obtenu une autorisation d'accès de la part du Comité sectoriel.

> Par exemple, par une décision du 6 novembre 2007, la section sécurité sociale du Comité sectoriel de la sécurité sociale a autorisé l'ONEm à obtenir notamment les informations relatives aux années de carrière des travailleurs salariés et aux nombres de jours de travail prestés durant ces années[105].

---

détentrice, les personnes auxquelles les données se rapportent, leurs représentants légaux et ceux qu'elles autorisent expressément à les traiter (1°) ; les personnes qui doivent traiter les données concernées en vue de remplir leurs obligations en matière de sécurité sociale, leurs préposés ou mandataires ainsi que celles qu'elles autorisent expressément à les traiter (2°) ; les personnes auxquelles des travaux en sous-traitance sont confiés par les personnes visées au 2°, en vue de l'application de la sécurité sociale (3°) ; les organismes de droit étranger, pour l'application des conventions internationales de sécurité sociale (4°) ; dans les cas déterminés par le Roi, les personnes qui réclament des données détenues par des institutions de sécurité sociale, leurs préposés ou mandataires ainsi que ceux qu'elles autorisent expressément à les traiter en vue de remplir leurs missions (5°). Précisons que cette dernière hypothèse est concrétisée par l'art. 3 de l'arrêté royal du 4 février 1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale qui prévoit notamment que le sous-traitant d'une institution peut obtenir communication des données détenues par cette dernière sans passer par la Banque-Carrefour.

[104] Art. 15 de la loi sur la Banque-Carrefour de la sécurité sociale. Sur les comités sectoriels, voy. *infra,* n°s 534.- et s.

[105] Comité sectoriel de la Sécurité sociale et de la Santé, section « sécurité sociale », délibération n° 07/063 du 6 novembre 2007 relative à la communication de données à caractère personnel par l'association sans but lucratif CIMIRe à l'Office National de l'Emploi et aux organismes de paiement des allocations de chômage, en vue du calcul informatisé du passé professionnel des assurés sociaux concernés.

Si l'information réclamée peut être fournie, la Banque-Carrefour vérifie qu'elle est *disponible* dans le réseau, grâce à la table des données disponibles. Celle-ci indique quelle donnée est disponible auprès de quelle institution de sécurité sociale du réseau primaire ou auprès de quel secteur de la sécurité sociale si l'information recherchée est détenue par une institution du réseau secondaire[106]. Remarquons que cette table des données disponibles n'est pas publique. Si un citoyen désire savoir quelles données de contenu sont détenues par les administrations avec lesquelles il a été ou est encore en contact, il doit contacter chacune d'elles séparément[107].

> Par exemple, pour chaque travailleur salarié, l'année de carrière, le salaire obtenu, le nombre de jours ou d'heures de travail prestés, le nombre moyen d'heures hebdomadaires prestées, etc. sont enregistrés dans la source authentique du CIMIRe qui est l'organisme compétent pour la collecte de données concernant la carrière professionnelle. Ainsi, si Monsieur Dupond a exercé un travail à temps plein en tant qu'assistant à l'université durant l'année 2008, il est enregistré dans la banque de donnée du CIMIRe qui reprend les données suivantes : Année de carrière : 2008 ; Salaire 23.884 euros ; Heures de travail : 1.656,80 h ; Nombre d'heures hebdomadaires : 38h ; Description : employé.

Si l'information est disponible dans le réseau primaire, la Banque-Carrefour se réfère au *répertoire des personnes* qui indique, pour chaque personne identifiée dans ce répertoire à l'aide de son numéro d'identification de sécurité sociale (en abrégé : NISS), auprès de quelle institution des informations la concernant sont disponibles, en quelle qualité[108] la personne est reprise dans la banque de données (cette caractéristique est appelée « code qualité »), et pour quelle période. Si l'information est disponible dans un réseau secondaire, l'institution de gestion de ce réseau doit intervenir en sus de la Banque-Carrefour afin de consulter son répertoire sectoriel de références et d'identifier l'institution du réseau secondaire détenant l'information recherchée.

> Par exemple, Monsieur Dupond, né le 17/09/1981 est engagé dans les liens d'un contrat de travail depuis le 01/01/2008 et est affilié à la mutualité

[106] F. Robben, « Le projet de loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale », *op. cit.,* p. 77.

[107] Voy. *infra,* n° 261.-, n° 294.-, n° 299.- et n° 383.-

[108] Dans le document que la Banque-Carrefour envoie lorsqu'un citoyen lui demande quelles sont les références que cette institution détient à son sujet, elle précise que « par qualité, il y a lieu d'entendre le type de dossier tenu à jour par une institution de sécurité sociale concernant une personne donnée. Il s'agit d'une notion purement factuelle qui a été créée par l'institution de sécurité sociale, dans le but d'une gestion plus efficace de ses dossiers, mais qui est dépourvue de toute conséquence juridique ».

Euromut. Il a également une télévision depuis le 01/04/2008. Il est repris dans le répertoire des personnes de cette façon :

NISS de Monsieur Dupond

ONSS- code qualité 010 – date de début 01/01/2008- sans date de fin. Cela signifie que l'ONSS gère un dossier relatif à Monsieur Dupond depuis son engagement professionnel. Le code 010 indique la qualité de « salarié ».

CIN (secteur mutualiste) –code qualité 001- date de début 17/09/1981- sans date de fin. Cela signifie que le Collège inter mutualiste National, qui est l'institution de gestion du réseau secondaire qu'est le secteur mutualiste, a géré un dossier pour Monsieur Dupond depuis sa naissance. Le code 001 indique la qualité « assurabilité soins de santé ». Le nom d'Euromut n'est donc pas repris dans le répertoire des références. Ainsi, on ne peut savoir, à la lecture de celui-ci, à quelle mutualité Monsieur Dupond est affilié.

CIMIRe – code qualité 030 – date de début 15/01/2008- date de fin 31/12/2007. Cela signifie que le CIMIRe a géré un dossier pour Monsieur Dupond durant cette période. Le code 030 indique la qualité de « travailleur pour qui une déclaration Dimona (déclaration immédiate à l'emploi) a été faite ».

Région wallonne – Cellule fiscale – code qualité 001- date de début 01/04/2008 – sans date de fin. Cela signifie que la Région wallonne- Cellule fiscale gère un dossier concernant Monsieur Dupond depuis cette date. Le code 001 indique la qualité « Radio Tv Redevance ».

c) L'acheminement de la donnée. Une fois que la Banque-Carrefour a trouvé la source authentique où se situe la donnée réclamée, elle demande directement à l'institution détentrice de la lui communiquer, s'il s'agit d'une institution du réseau primaire. Si la donnée se situe auprès d'une institution du réseau secondaire, la Banque-Carrefour réclame la donnée à l'institution de gestion du réseau secondaire, chargée notamment d'assurer les communications de données entre les institutions du réseau secondaire et la Banque-Carrefour[109]. Les institutions de sécurité sociale sollicitées transmettent alors les données réclamées à la Banque-Carrefour, comme les y oblige la loi[110]. Finalement, une fois en possession de la donnée demandée, la Banque-Carrefour la transmet à l'institution demanderesse[111].

Par exemple, en 2009, Monsieur Dupond est mis au chômage. En vue du paiement des allocations, l'ONEm et les organismes de paiement des allocations

[109] Art. 6 de l'arrêté royal du 4 février 1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale, *M.B.,* 3 avril 1997.

[110] Art. 10 de la loi sur la Banque-Carrefour de la sécurité sociale.

[111] Pour plus de précisions, voy. V. VERDEYEN, « Informatisation de la sécurité sociale », *in La Sécurité sociale en pratique,* Bruxelles, Kluwer, 2009, spéc. pp. 16 et 17 qui concernent la mise à jour des informations acheminées.

de chômage ont demandé à la Banque-Carrefour certaines informations nécessaires pour établir le passé professionnel de Monsieur Dupond, telles que ses années de carrière et le nombre de jours de travail prestés durant ces années. Grâce à la consultation de la table des données disponibles, la Banque-Carrefour a identifié que les données réclamées sont enregistrées par le CIMIRe. Elle achemine donc la demande de données relatives aux années de carrières et au nombre de jours de travail prestés durant ces années au CIMIRe. Celui-ci consulte sa banque de données, et transmet les données suivantes à la Banque-Carrefour : *Année de carrière :* 2006 ; *Heures de travail* : 1.656,80 h ; *Nombre d'heures hebdomadaires* : 38h[112]. La Banque-Carrefour achemine ensuite ces données vers l'ONEm et les organismes de paiement des allocations de chômage.

C. Le numéro d'identification

26.- Considérations générales. La circulation des données personnelles dans l'administration suppose que chaque individu soit identifié de manière unique et fiable, ce qui se fait grâce à l'utilisation d'un numéro d'identification. Après avoir défini cet outil et expliqué sa raison d'être, le numéro d'identification du Registre national illustre nos propos.

§1. Définition et raison d'être

27.- Définition. Le numéro d'identification d'un citoyen est un ensemble de chiffres, auquel sont parfois jointes des lettres, qui est attribué à un seul individu, et dont la fonction est l'identification fiable de cette personne lors de l'accomplissement d'une tâche administrative[113] telle que l'enregistrement de l'individu dans une base de données, la consultation d'une source authentique de données, l'échange de données entre différentes autorités.

28.- Raison d'être. L'attribution, à chaque citoyen, d'un numéro, plutôt que l'utilisation de ses nom et prénoms pour l'identifier, est justifiée

[112] Pour obtenir le nombre de jours de travail prestés, il faut diviser le nombre total d'heures effectuées par le nombre d'heures hebdomadaires. On obtient le nombre de semaines effectuées dans l'année. Ce nombre multiplié par 6 donne le nombre de jours de travail en équivalent temps plein et converti en un régime de 6 jours/semaine [Information complémentaire fournie par le CIMIRe dans le document joignant l'extrait global de carrière que le CIMIRe envoie aux citoyens lorsqu'ils le demandent].

[113] Le numéro d'identification peut également être utilisé dans le secteur privé. Toutefois, ainsi qu'on l'a précisé dans l'introduction de la recherche, nous nous concentrons sur l'utilisation du numéro d'identification dans le secteur public, à des fins administratives.

par le souci d'éviter toute confusion entre les personnes lors du traitement de leur dossier.

Ce souci est d'autant plus important que les citoyens sont de plus en plus nombreux. Ils sont également de plus en plus fréquemment amenés à être en contact avec l'État, depuis le développement de l'État-providence principalement[114]. Dans un tel contexte, les nom et prénoms, par exemple, seraient insuffisants pour éviter de confondre plusieurs individus, étant donné que beaucoup de personnes portent le même nom et que, suivant les modes, les mêmes prénoms sont octroyés[115].

Ainsi, grâce à cet instrument, une administration qui consulte une source authentique peut se contenter d'introduire le numéro d'identification de l'individu dont elle traite le dossier pour voir apparaître sur l'écran les données de cette seule personne. Lorsqu'une administration doit faire parvenir des informations relatives à un citoyen à une autre institution, il lui suffit de mentionner le numéro d'identification de ce dernier ; il est alors certain que l'institution recevant le dossier saura de quel unique individu il s'agit. L'efficacité administrative est renforcée.

§2. L'exemple du numéro d'identification du Registre national

29.- Un numéro d'identification. Le numéro d'identification du Registre national, est, comme son nom l'indique, un numéro d'identification attribué à toute personne inscrite au Registre national, et ce, dès la première inscription[116]. Sa composition en fait un numéro signifiant.

---

[114] Voy. *infra,* n°s 46.-et s.

[115] Conseil de l'Europe, Les numéros personnels d'identification : leur mise en œuvre, leur utilisation et la protection des données, 1991, p. 8 disponible sur le site :

httphttp://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/rapports_et_%E9tudes_des_comit%E9s_de_protection_des_donn%E9es/X-Pins_1991.asp#TopOfPage

[116] Art. 2, al. 2, de la loi du 8 août 1983 sur le Registre national. Certaines personnes ne sont pas enregistrées au Registre national mais sont néanmoins amenées à être en contact avec des administrations belges, telles que les administrations de sécurité sociale. C'est le cas, par exemple, des personnes vivant à l'étranger mais travaillant en Belgique. Les données d'identification de ces personnes sont enregistrées dans une base de données détenue par la Banque-Carrefour de la sécurité sociale, qui fait office de source d'identification complémentaire au Registre national. Ces personnes sont identifiées au sein de l'Administration à l'aide de leur numéro d'identification de la Banque-Carrefour de la sécurité sociale, dit aussi « numéro bis » [art. 8, 2°, de la loi du 15 janvier 1990 susvisée]. Ce numéro est composé de la manière définie par l'arrêté royal du 8 février 1991 relatif à la composition et aux modalités d'attribution du numéro d'identification des personnes physiques qui ne sont pas inscrites au Registre national des personnes physiques.

L'utilisation qui en est faite aujourd'hui lui confère la qualité de numéro unique d'identification.

30.- La composition du numéro d'identification du Registre national. La composition du numéro d'identification du Registre national est déterminée par le Roi, auquel cette tâche a été déléguée par le législateur[117].

Ainsi, un arrêté royal du 3 avril 1984[118] prévoit que ce numéro est composé de onze chiffres, divisés en trois groupes.

Le premier groupe est constitué de six chiffres qui représentent, en principe[119], la date de naissance en sens inverse.

Le deuxième groupe est constitué de trois chiffres appelés « le numéro d'ordre ». Ils correspondent au rang d'inscription de la personne dans le compteur journalier des naissances. Ils révèlent également le sexe de l'individu puisqu'il est pair si la personne est de sexe féminin et impair si la personne est de sexe masculin.

Le troisième et dernier groupe est composé de deux chiffres et constitue le « numéro de contrôle ». Il représente le quotient d'une division effectuée à partir des neuf premiers chiffres[120].

Ce numéro est donc signifiant en ce qu'il permet de connaître, à sa seule lecture, la date de naissance et le sexe de la personne concernée, ce qui est problématique. Indépendamment des questions relatives à la protection de la vie privée sur lesquelles nous reviendrons[121], la mention du sexe dans le numéro d'identification est critiquée[122]. En effet, certains citoyens changent de sexe au cours de leur vie. Il y a dès lors lieu d'adapter leur numéro d'identification en conséquence. Cela pose problème compte tenu du fait que le numéro d'identification du Registre national est présent dans un grand nombre de bases de données, qu'il faut donc également modifier,

---

[117] Art. 2, al. 2, de la loi du 8 août 1983 sur le Registre national.

[118] Arrêté royal du 3 avril 1984 relatif à la composition du numéro d'identification des personnes inscrites au Registre national des personnes physiques, *M.B.,* 21 avril 1984.

[119] L'art. 5 de cet arrêté royal prévoit une composition particulière pour le premier groupe de chiffres dans l'hypothèse ou le jour ou le mois de naissance d'une personne ne sont pas connus ou si les numéros d'ordre pairs ou impairs pour une date de naissance déterminée sont épuisés.

[120] Art. 1 et 4 de l'arrêté royal du 3 avril 1984 susvisé.

[121] Voy. *infra,* n° 196.-

[122] Cette mention suscite la désapprobation de la CPVP (voy. avis n° 30/98 du 25 septembre 1998 relatif au Registre national, p. 4, n° 3 ; CPVP, avis n° 12/2003 du 13 janvier 2003, relatif au projet d'arrêté royal déterminant les informations techniques associées aux informations visées à l'art. 3, al. 1er, de la loi du 8 août 1983 organisant un registre national des personnes physiques, pp. 2 et 3).

ce qui entraîne « des erreurs de traitement de ce numéro »[123]. C'est pourquoi, selon la CPVP[124], le numéro d'identification du Registre national ne devrait pas avoir de contenu spécifique mais être composé d'une manière aléatoire, afin de ne pas devoir être modifié après son attribution.

Néanmoins, le législateur a estimé, il y a quelques années[125], que la transformation de ce numéro en un numéro non-signifiant entraînerait trop de charges pour les gestionnaires des nombreux fichiers dans lesquels se trouvent ce numéro, utilisé depuis les années septante et ayant parfois même servi de base au développement de certains fichiers. Il a, dans le même temps, affirmé son intention d'évoluer « prochainement vers un numéro national ne contenant plus de données à caractère personnel »[126], ce que l'on attend toujours.

31.- L'utilisation du numéro d'identification du Registre national. L'utilisation du numéro d'identification du Registre national n'est pas libre. Elle est soumise au respect de trois conditions.

Premièrement, seules les institutions limitativement énumérées par la loi du 8 août 1983 sur le Registre national peuvent demander l'autorisation de l'utiliser[127].

> En effet, en vertu des articles 5 et 8 de la loi du 8 août 1983 sur le Registre national, l'autorisation d'utiliser ce numéro d'identification ne peut être octroyée qu' :
>
> « 1° aux autorités publiques belges pour les informations qu'elles sont habilitées à connaître en vertu d'une loi, d'un décret ou d'une ordonnance ;
>
> 2° aux organismes publics ou privés de droit belge pour les informations nécessaires à l'accomplissement de tâches d'intérêt général qui leur sont confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ou de tâches reconnues explicitement comme telles par le comité sectoriel précité ;

[123] CPVP, avis n° 30/98, *op. cit.,* p. 2 ; CPVP, avis n° 12/2003, *op. cit.,* p. 3.

[124] CPVP, avis n° 12/2003, *op. cit.,* p. 3.

[125] Projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques, *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50 2226/001, pp. 6-7.

[126] Projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques, *op. cit.,* p.7.

[127] L'octroi de cette autorisation est de la compétence du Comité sectoriel du Registre national (art. 8 de la loi du 8 août 1983 sur le Registre national).

3° aux personnes physiques ou morales qui agissent en qualité de sous-traitants des autorités publiques belges et des organismes publics ou privés de droit belge visés aux 1° et 2°; l'éventuelle sous-traitance se fait à la demande, sous le contrôle et sous la responsabilité desdits autorités et organismes ; ces sous-traitants doivent s'engager formellement à respecter les dispositions de la présente loi et de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et prennent les mesures nécessaires à cette fin, dont ils font état aux personnes pour lesquelles ils agissent en qualité de sous-traitants ;

4° aux notaires et aux huissiers de justice pour les informations qu'ils sont habilités à connaître en vertu d'une loi, d'un décret ou d'une ordonnance ;

5° à l'Ordre des pharmaciens dans le but de communiquer à leurs membres la résidence principale d'un client auquel un médicament dangereux pour la santé aurait été remis ;

6° à l'Ordre des barreaux francophones et germanophone et l'*Orde van de Vlaamse balies*, dans le seul but de communiquer aux avocats les informations dont ils ont besoin pour les tâches qu'ils remplissent en tant qu'auxiliaires de la justice ».

En d'autres termes, une société privée, par exemple, ne peut utiliser le numéro d'identification du Registre national dans le cadre de ses activités lucratives[128].

Deuxièmement, ces autorités ne peuvent utiliser ce numéro que dans le but d'exercer les missions qui – en substance – leur ont été confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance, et ce, en vertu de l'article 5 de cette loi également.

Troisièmement, elles doivent avoir été autorisées à utiliser ce numéro par le Comité sectoriel du Registre national[129].

D'autres conditions d'utilisation du numéro d'identification du Registre national sont prévues dans des lois plus récentes. Ces lois ne complètent

[128] La violation d'une telle interdiction peut entraîner une condamnation judiciaire. À cet égard voy. E. Degrave, « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données illégal sanctionné par la Cour d'appel de Bruxelles », obs. sous Bruxelles (9e ch.), 9 mai 2012, *J.T.,* 2012, pp. 691 à 693.

[129] Art. 8 de la loi du 8 août 1983 sur le Registre national *Voy. infra,* nos 534.-et s. La procédure d'autorisation par le Comité sectoriel du registre national remplace la procédure d'autorisation par arrêté royal, depuis la loi du 25 mars 2003 modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.,* 28 mars 2003. Sur l'utilisation du numéro d'identification du Registre national par une entreprise privée en relation avec une institution de sécurité sociale, voy. K. Rosier, « Le numéro d'identification du registre national : une donnée pas comme les autres », *Bull. Soc.,* 2007, p. 6.

pas la loi sur le Registre national mais prévoient une autre réglementation pour l'utilisation de ce numéro, propre au secteur dans lequel il est utilisé.

> Ainsi, par exemple, la *loi relative à la Banque-Carrefour de la sécurité sociale* prévoit que, « pour l'accomplissement de ses missions, la Banque-Carrefour peut utiliser le numéro d'identification du Registre national »[130]. En d'autres termes, cette institution peut utiliser ce numéro sans devoir, notamment, demander l'autorisation au Comité sectoriel du Registre national. Lors des discussions préparatoires à l'adoption de ce texte, la section de législation du Conseil d'État a pourtant affirmé qu'« en l'espèce, rien ne paraît justifier une dérogation à [la] règle [prévue par les articles 5 et 8 de la loi sur le Registre national] », que « le projet ne met d'ailleurs pas de restriction au droit d'utiliser le numéro d'identification » alors que lorsque cette utilisation est autorisée, « elle est assortie conformément à l'article 8 de la loi du 8 août 1983, de l'indication des limites assignées à ce droit d'utilisation »[131]. Néanmoins, la règle n'a pas été changée.
>
> Le *Code des impôts sur les revenus 1992* règle également l'utilisation de ce numéro d'identification de manière particulière[132]. La CPVP s'est exprimée à ce sujet en affirmant que « s'il est évident que le Législateur peut accorder l'autorisation à quiconque, de faire usage du numéro d'identification, [elle] aurait souhaité [...] que cette autorisation respecte les conditions de l'article 8 de la loi du 8 août 1983 et précise pour chaque autorité ou organisme, les modalités d'utilisation du numéro ». Elle regrette que cette réglementation aboutisse à « faire échapper du champ d'application de la loi du 8 août 1983 l'exécution des lois et règlements relatifs aux impôts sur les revenus et contribue, à terme, à dénaturer le système de protection de la vie privée prévu lors de la création du Registre national »[133].

Finalement, malgré le fait que l'utilisation du numéro de Registre national soit encadrée par la loi, elle est largement répandue au sein des administrations qui l'utilisent pour servir des fonctions différentes. Ce numéro ne sert pas seulement à la gestion du Registre national mais est également utilisé, par exemple, comme numéro fiscal[134], comme numéro d'identifi-

---

[130] Art. 7, 2°, de ladite loi.

[131] Avis S.L.C.E. relatif au projet de loi relatif à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *Pasin.,* 1990, I, p. 105.

[132] Art. 314, §3, C.I.R. 92.

[133] CPVP, avis n° 22/93, du 6 décembre 1993, relatif au projet de loi modifiant l'art. 314 du Code des impôts sur les revenus (C.I.R.) 1992. Utilisation du numéro fiscal d'identification des personnes physiques, p. 5, n°s 8 et 9. Voy. également, à propos d'une modification du C.I.R. 92 par un arrêté royal, l'avis n° 24/93 du 6 décembre 1993 relatif au projet d'arrêté royal modifiant, en ce qui concerne l'obligation de fournir le numéro fiscal d'identification, l'arrêté royal C.I.R. 92.

[134] Art. 314, §1, al. 1 et 2, C.I.R 92 : « L'administration des contributions directes attribue un numéro fiscal d'identification aux contribuables soumis aux impôts visés à l'art. 1er ». « Pour les personnes physiques, ce numéro fiscal correspond à leur numéro d'identification dans le Registre national des personnes physiques ».

cation de la sécurité sociale[135] et comme numéro d'identification pour les échanges de données transitant par l'intégrateur de services fédéral[136].

L'utilisation de ce numéro d'identification risque encore de s'étendre. En effet, la CPVP encourage une plus grande libéralisation de ce numéro, du moins pour les administrations n'utilisant pas des données dites « sensibles »[137], en prônant une interprétation souple de la procédure d'autorisation « compte tenu du caractère limité du danger d'utiliser le numéro du Registre national »[138]. Ainsi soutient-elle que le droit d'obtenir l'accès au Registre national doit entraîner d'office le droit d'utiliser le numéro. Il doit également être possible d'obtenir l'utilisation dudit numéro alors même que l'accès à la source authentique ne serait pas demandé ou serait refusé. En outre, le bénéficiaire d'une autorisation peut utiliser le numéro pour la gestion interne de son administration mais également dans ses rapports avec les tiers pour l'exécution de ses tâches légales. Ces derniers acquièrent alors « automatiquement » le droit d'utiliser ledit numéro dans leurs relations avec les citoyens concernés[139].

II. De nouvelles opérations

32.- L'octroi d'avantages et le renforcement du contrôle. Grâce au développement de l'e-gouvernement fondé sur l'utilisation d'outils nouveaux tels que les sources authentiques de données, les plateformes

[135] Art. 8 §1 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale : « Lors du traitement de données en application de la présente loi et de ses arrêtés d'exécution, seuls les identifiants suivants sont utilisés : 1° le numéro d'identification du Registre national s'il s'agit de données relatives à une personne physique enregistrée dans ledit registre » ; Art. 1, 4°, de l'arrêté royal du 18 décembre 1992 : « Il faut entendre par 'numéro d'identification de la sécurité sociale' : le numéro d'identification du Registre national s'il s'agit d'un assuré social repris dans ledit Registre [...] ».

[136] Art. 5 de la loi du 15 août 2012 sur l'intégrateur de services fédéral.

[137] Lorsqu'il s'agit d'assurer l'échange de données sensibles, au sens de l'art. 8 de la loi du 8 décembre 1992, telles que des données relatives à la santé, par exemple, la CPVP encourage la création de numéros d'identification sectoriels, spécifiquement réservé au traitement de données à caractère personnel dans le domaine de la santé ou de la justice [Voy. l'avis n° 14/2002, du 8 avril 2002, relatif au projet d'arrêté royal fixant les normes auxquelles le programme de soins de base en oncologie et le programme de soins d'oncologie doivent répondre pour être agréés, p. 4, n° 8 ; avis n° 19/2002, *op. cit.,* p. 10, n° 19 ; avis n° 01/2005, du 10 janvier 2005, relatif au projet d'arrêté royal organisant l'enregistrement du cancer, pp. 5 et 6 ; avis n° 13/2006, du 24 mai 2006, relatif à l' identification et signature électronique au sein du système d'information Phenix, p. 6, n° 26.

[138] CPVP, avis n° 30/98, *op. cit.,* p. 5, n° 2.

[139] CPVP, avis n° 28/1999 relatif à un avant-projet de loi modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques, p. 5 ; CPVP, avis n° 30/98, *op. cit.,* p. 5, n° 2 ; CPVP, avis n° 19/2002, *op. cit.,* p. 9, n° 17.

d'échange d'informations et les numéros d'identification, des opérations nouvelles peuvent être menées au sein du secteur public.

Entre autres possibilités, l'administration peut aujourd'hui octroyer automatiquement certains droits, comme le tarif social lors de la fourniture de gaz et d'électricité. Elle peut également exercer davantage de contrôle sur les citoyens. L'exemple du profilage est, à cet égard, très parlant.

A. L'octroi d'avantages aux citoyens : l'automatisation des droits

33.- Considérations générales. Grâce aux transferts de données entre administrations, il est à présent possible d'octroyer automatiquement certains droits à ceux qui peuvent en bénéficier. Par exemple, l'octroi du tarif social en matière de gaz et d'électricité est automatisé.

§1. Définition et raison d'être

34.- Définition. L'automatisation d'un droit peut être définie comme une opération menée dans le but d'octroyer un droit aux personnes bénéficiaires, sans que celles-ci doivent le demander ou prouver qu'elles remplissent les conditions d'octroi de ce droit.

Cette opération est fondée principalement sur l'échange, au sein de l'administration, d'informations issues de sources authentiques distinctes, transitant par une plateforme d'échanges d'informations.

35.- Raison d'être. L'automatisation des droits tend à se généraliser dans l'administration.

À l'appui de cette extension, on avance *l'intérêt des bénéficiaires de ces droits*. Ceux-ci font généralement partie d'une catégorie vulnérable de la société qui n'a pas nécessairement conscience de ces avantages.

En ce sens, « l'informatisation accentuée et le croisement optimal des informations sociales doit [...] permettre [...] à l'Administration de débusquer les nids de pauvreté cachés, dans le chef des personnes qui ne font pas appel, par ignorance, aux mécanismes de protection sociale que la loi leur assure »[140]. Parfois, bien que pensant à réclamer de tels droits, les personnes concernées échouent dans leur démarche à défaut d'avoir pu fournir les attestations nécessaires pour prouver leur situation.

[140] Rapport fait au nom de la Commission des affaires sociales par Mme NELIS-VAN LIEDEKERKE relatif au projet de loi relatif à l'institution et à l'organisation d'une Banque carrefour de la sécurité sociale, publié dans *Pasin.,* 1990, I, p. 117.

Actuellement, la mise en place de ce nouveau type d'opération concerne principalement l'octroi des droits en matière de sécurité sociale[141], conformément à ce qui avait été annoncé dès la création de la Banque-Carrefour de la sécurité sociale et qui a été réitéré par la suite[142].

On invoque également le fait que l'envoi d'attestations représente un *coût budgétaire* non négligeable qui pourrait être diminué si ces envois étaient remplacés par la consultation de sources authentiques et l'échange électronique des informations requises[143].

---

[141] À cet égard, le Comité sectoriel de la Sécurité sociale et de la Santé, section « Sécurité sociale a déjà rendu plusieurs décisions en vue de l'automatisation de certains droits sociaux. Voy. notamment, en ce qui concerne l'octroi automatique de certains avantages fiscaux aux personnes handicapées, la délibération n° 08/004 du 15 janvier 2008 relative à la communication de certaines données à caractère personnel à l'entité impôts et recouvrement du Service Public Fédéral Finances ; en ce qui concerne l'octroi automatique d'un tarif téléphonique social à certaines catégories de personnes socialement défavorisées, la délibération n° 06/015 du 7 mars 2006 relative à la communication de données à caractère personnel à l'IBPT, en vue de l'octroi d'un tarif téléphonique social ; en ce qui concerne l'exemption automatique de la redevance sur la pollution des eaux à certaines catégories de personnes socialement défavorisées, la délibération n° 05/005 du 18 janvier 2005 relative à la communication de données à caractère personnel aux sociétés de distribution d'eau compétentes [...].

[142] Ainsi, lors de l'élaboration de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque carrefour de la sécurité sociale, il a été affirmé que « à terme, la réforme proposée permettra même, dans un certain nombre de cas, de substituer à l'obligation pour les assurés sociaux de demander le bénéfice d'un droit social, une obligation pour les organismes de sécurité sociale d'examiner ces droits d'initiative, sur al base de l'information disponible dans le réseau et d'éventuellement les octroyer d'office » [Exposé des motifs du projet de loi relatif à l'institution et à l'organisation d'une Banque carrefour de la sécurité sociale, publié dans *Pasin.,* 1990, I, p. 78].

Dans le même sens, le Ministre de l'Emploi et de l'informatisation de l'État, Peter Vanvelthoven, affirmait il y a quelques années sa volonté de « poursuivre la généralisation de l'octroi automatique de droits sociaux ou d'avantages supplémentaires sur la base du statut social » [P. VANVELTHOVEN, « Aperçu de la situation actuelle en matière d'E-government dans le secteur social », 28 août 2006, disponible sur le site http://www.ksz.fgov.be/documentation/fr/documentation/Presse/Rencontre_de_presse_240806.ppt#256,1, Aperçu de la situation actuelle en matière d'E-government dans le secteur social, p. 32].

[143] Projet de loi-programme, Rapport fait au nom de la Commission des affaires sociales par M. Bernard BAILLE, *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50 2343/017, p. 18 ; Amendement n° 26 au projet de loi-programme, Justification, *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50 2343/010, p. 2 ; Amendement n° 1 au projet de loi-programme, Justification, *Doc. Parl.,* Ch. Repr., sess. 2006-2007, n° 51 3058/005, p. 7 ; Projet de loi-programme, Exposé introductif de M. VERWILGHEN, *Doc. Parl.,* Ch. Repr., sess. 2006-2007, n° 51 3058/012, p. 6.

§2. L'exemple du tarif social pour la fourniture d'électricité et de gaz naturel

36.- L'octroi automatique d'un tarif préférentiel. Les personnes socialement défavorisées qui ont, de ce fait, un statut particulier en matière de sécurité sociale – telles que les bénéficiaires d'un revenu d'intégration accordé par un CPAS ou de certaines allocations octroyées aux personnes handicapées – peuvent bénéficier d'un tarif social pour la fourniture de gaz et d'électricité, appelé également « prix maximaux sociaux »[144].

Il y a quelques années encore, pour bénéficier de ce droit, les personnes concernées devaient prendre l'initiative de le demander. Elles devaient également fournir les attestations nécessaires pour prouver leur statut en matière de sécurité sociale.

Aujourd'hui, la loi-programme du 27 avril 2007 organise « l'application automatique de prix maximaux pour la fourniture d'électricité et de gaz naturel aux clients protégés résidentiels à revenus modestes ou à situation précaire ». En d'autres termes, cette loi organise l'application automatique du tarif social aux personnes qui peuvent en bénéficier[145]. Ces dernières ne doivent donc plus demander le bénéfice de cet avantage et ne doive plus prouver leur statut.

L'organisation de cette automatisation par une loi a été jugée « nécessaire pour trois raisons : elle offre la possibilité au SPF Economie d'avoir accès au registre national des personnes physiques et au registre de la Banque-Carrefour de la sécurité sociale ; il organise et coordonne l'échange de données entre la Banque-Carrefour de la sécurité sociale, les fournisseurs et les gestionnaires de réseau ; il fixe les cas où la remise d'une attestation reste tout de même d'application »[146].

L'automatisation du droit à un tarif social lors de la fourniture de gaz et d'électricité est rendue possible grâce à la collaboration du SPF Economie,

---

[144] Voy. la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité, *M.B.*, 11 mai 1999 ; la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisation, *M.B.*, 7 mai 1965 ; l'arrêté royal du 30 mars 2007 portant fixation de prix maximaux sociaux pour la fourniture d'électricité aux clients protégés à revenus modestes ou à situation précaire, *M.B.*, 6 juillet 2007 ; l'arrêté ministériel du 30 mars 2007 portant fixation de prix maximaux sociaux pour la fourniture de gaz aux clients résidentiels protégés à revenus modestes ou à situation précaire, *M.B.*, 19 juin 2007.

[145] Loi-programme du 27 avril 2007, *M.B.*, 8 mai 2007. Cette loi est en vigueur depuis le 1er juillet 2009 (arrêté royal du 28 avril 2010 relatif à la date d'entrée en vigueur des articles 3 à 11 de la loi-programme du 27 avril 2007, *M.B.*, 18 mai 2010).

[146] Exposé introductif de M. VERWILGHEN, *Doc. Parl.*, Ch. Repr., sess. 2006-2007, n° 51 3058/012, p. 7.

de la Banque-Carrefour de la Sécurité sociale, et des fournisseurs d'énergie et gestionnaires de réseau de distribution.

37.- La centralisation de données au SPF Economie. Une base de données est créée au sein du SPF Economie, qui contient des données d'identification de toutes les personnes achetant du gaz et de l'électricité pour leur propre usage. Ces informations sont communiquées par les fournisseurs d'énergie et les gestionnaires de réseau de distribution. Il s'agit, principalement, des nom, prénom, adresse de la résidence principale, adresse de raccordement pour la fourniture d'électricité et de gaz, de l'entièreté de leur clientèle[147].

Cette banque de données doit être utilisée exclusivement dans le but de permettre l'octroi automatique du tarif social pour l'électricité et le gaz[148].

Néanmoins, suite à l'avis de la CPVP[149], le législateur a explicitement prévu le droit, pour toute personne concernée, de « s'opposer gratuitement au traitement des données relatives à sa personne [...] moyennant une notification afférente datée et signée adressée à son fournisseur »[150]. Si une personne fait usage de ce droit, le fournisseur ne communiquera pas ses données personnelles au SPF Economie et la personne devra demander l'octroi de ce droit en fournissant les attestations nécessaires[151].

38.- L'identification des bénéficiaires par la Banque-Carrefour de la sécurité sociale. Pour identifier les bénéficiaires du tarif social parmi les nombreuses personnes enregistrées dans la base de données du SPF Economie, ce dernier doit s'adresser à la Banque-Carrefour de la sécurité

[147] L'article 8 de ladite loi prévoit que les fournisseurs communiquent « le nom, le prénom et l'adresse de la résidence principale des clients finals, la date d'entrée en vigueur de leur contrat de fourniture, leur code EAN et leur adresse de raccordement pour la fourniture d'électricité et de gaz naturel ainsi que, le cas échéant, leur date de naissance ». Les gestionnaires de réseau de distribution fournissent « les codes EAN et les adresses de raccordement pour la fourniture d'électricité et de gaz naturel de tous les clients finals ».

[148] Art. 5 de la loi-programme ; Voy. égal. la justification de l'amendement n° 1 au projet de loi-programme, *Doc. Parl.*, Ch. Repr., sess. 2006-2007, n° 51 3058/005, p. 9 ; CPVP, avis n° 11/2007 du 21 mars 2007 relatif à un avant-projet de loi réglant l'application automatique de prix maximaux pour la fourniture d'électricité et de gaz naturel aux clients protégés résidentiels à revenus modestes ou à situation précaire, p. 3, n° 10.

[149] CPVP, avis n° 11/2007, *op. cit.*, p. 4, n° 11.

[150] Art. 6, al. 3, de la loi-programme.

[151] Justification de l'amendement n° 1 au projet de loi-programme, *op. cit.*, p. 10.

sociale. Il est d'ailleurs obligé de le faire, en vertu de l'article 11*bis* de la loi sur la Banque-Carrefour de la Sécurité sociale[152].

À partir des données disponibles dans le réseau de la sécurité sociale, la Banque-Carrefour identifie les personnes dont le statut en matière de sécurité sociale justifie l'octroi du tarif social. Pour faciliter ce travail, la Banque-Carrefour peut enregistrer dans son répertoire des personnes le numéro d'identification de la sécurité sociale de chaque personne qui achète du gaz et de l'électricité et dont les données lui ont été communiquées par le SPF Economie[153]. Dès que les identifications sont effectuées, la Banque-Carrefour communique la liste des bénéficiaires au SPF Economie.

39.- La communication des bénéficiaires aux fournisseurs d'énergie. Finalement, une fois en possession de la liste des personnes pouvant obtenir le tarif social, le SPF Economie communique à chaque fournisseur le nom et le code EAN de leur client, assorti de la mention selon laquelle ce client a droit, ou non, à l'application du tarif social pour la fourniture d'électricité et de gaz naturel. Le SPF Economie doit être attentif à ce que chaque fournisseur ne reçoive que les données de ses propres clients[154]. À partir de ces informations, les fournisseurs d'énergie appliquent automatiquement le tarif social aux personnes concernées.

B. Le contrôle des citoyens : le profilage

40.- Considérations générales. Dans l'e-gouvernement, un contrôle efficace des citoyens peut être organisé, notamment parce que des technologies offrent de puissantes capacités de calculs permettant des opérations de profilage, définies et illustrées ci-après.

---

[152] En effet, l'octroi du tarif social lors de la fourniture de gaz et d'électricité est un « droit supplémentaire », au sens de cette disposition. En outre, le législateur semble considérer, en l'espèce, que le SPF Economie, *in*tervenant au nom des fournisseurs d'énergie et des gestionnaires de réseau, est une « instance d'octroi » au sens de cette disposition [Amendement n° 1 au projet de loi-programme, Justification, *Doc. Parl.,* Ch. Repr., sess. 2006-2007, n° 51 3058/005, p. 9]. Par ailleurs, précisons que cette obligation ne dispense pas le SPF Economie d'obtenir, préalablement au traitement des informations, l'autorisation du Comité sectoriel de la sécurité sociale et de la santé, section « sécurité sociale ». Dans le même sens, pour pouvoir utiliser le numéro d'identification du Registre national dans ses relations avec la Banque-Carrefour, le SPF Economie doit obtenir l'autorisation du comité sectoriel du Registre national (art. 7, al. 2, de la loi-programme).

[153] Art. 9, al. 2, de la loi-programme.

[154] Art. 10, §2, de la loi-programme.

§1. Définition et raison d'être

41.- Définition. Le Conseil de l'Europe définit le profilage comme « une technique de traitement automatisé des données qui consiste à appliquer un 'profil' – c'est-à-dire, un ensemble de données qui caractérisent une catégorie d'individus- à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels »[155].

En d'autres termes, le profilage consiste à soumettre les données à caractère personnel du citoyen à un logiciel de calculs, capable d'effectuer notamment des comparaisons et des corrélations statistiques. En fonction du résultat de ces calculs, l'individu est rattaché à une catégorie prédéterminée de la population, qui présente des caractéristiques spécifiques justifiant qu'on lui réserve une attitude particulière, comme, par exemple, une inspection fiscale pour les fraudeurs fiscaux présumés[156].

> Prenons un exemple qui, pour la clarté de l'exposé, simplifie à l'extrême cette technique très complexe. John a 30 ans et est chercheur à l'Université de Namur. Les données fiscales à son sujet révèlent qu'il perçoit un maigre salaire. Statistiquement, il devrait faire partie de la catégorie des citoyens ayant une petite voiture et une habitation modeste. Or, les données de la DIV montrent que John roule dans une BMW neuve. Le Registre national indique que son domicile est situé à Lasne, et il ressort des données fiscales que le précompte immobilier de son habitation est élevé. John serait-il coupable de fraude sociale ou fiscale ? En tout cas, la méfiance est de mise. John est rattaché à la catégorie des présumés fraudeurs fiscaux et sociaux et un contrôle fiscal et/ou social sera encouragé.

42.- Raison d'être. Dans l'e-gouvernement, le recours au profilage est motivé par la volonté d'augmenter l'efficacité administrative. Les discussions parlementaires relatives à un projet de loi organisant le profilage

---

[155] Recommandation CM/Rec(2010)13 du Comité des Ministres du Conseil de l'Europe aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, disponible sur le site www.coe.int

[156] M. Hildebrandt, « Who is Profiling Who ? Invisible Visibility », *in Reinventing Data Protection ?* (S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne et S. Nouwt éd.), Dordrecht, Springer, 2009, p. 241 ; V. Papakonstantinou, « A Data Protection Approach to Data Matching Operations Among Public Bodies », *International Journal of Law and Information Technology,* 2001, vol. 9, n° 1, pp. 62-63 ; J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, « L'application de la Convention 108 au mécanisme de profilage. Eléments de réflexion destinés au travail futur du Comité consultatif », mars 2008, T-PD (2008) 01, p. 5.

en matière fiscale[157] l'affirment d'emblée en soutenant que « le *datamining*[158] doit permettre de détecter le risque de fraude chez les contribuables et de déterminer ainsi, d'une manière plus efficace, les contribuables à contrôler »[159].

Cette technique permet de passer en revue une masse importante de citoyens, compte tenu de l'énorme quantité de données qui peut être absorbée par les outils informatiques dédiés à cette technique. En outre, le profilage permet de faire ressortir les individus à qui, concrètement, un traitement particulier doit être réservé. Cette identification est faite de manière plus fine que si elle était réalisée par des agents de l'administration, car l'outil de profilage peut traiter un nombre gigantesque de données et effectuer de multiples corrélations entre celles-ci. Ce faisant, il y a ainsi une forte présomption que l'individu qui a été rattaché à un profil par la technique du profilage, présente, concrètement, les caractéristiques de ce profil définies abstraitement[160]. La technique du profilage est également plus rapide, et donc moins couteuse, que la sollicitation des agents.

§2. L'exemple du profilage au service de la lutte contre la fraude sociale

43.- La sécurité sociale, le profilage et OASIS. La technique du profilage est utilisée dans l'administration, notamment pour lutter contre les fraudes à la législation sociale. Pour ce faire, un entrepôt de données qui répond au nom exotique de « OASIS »[161] a été créé. Il regroupe un grand nombre de données servant de base aux opérations de profilage.

---

[157] Ce projet de loi est devenu la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions, *M.B.,* 24 août 2012.

[158] Le « *datamining* » signifie « exploration de données », qui est une étape de l'opération de profilage.

[159] Projet de loi portant des dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions, Exposé des motifs, *Doc. Parl.,* Ch. Repr., session 2011-2012, n° 53-2343/001, p. 5. Au sujet de ce projet de loi, voy. E. Degrave et Y. Poullet, « Entre chasse à la fraude et respect de la vie privée », *Le Soir,* 4 mai 2012.

[160] M. Saintrain, « TIC, nouveaux standards transactionnels et fiscalité », Bureau du Plan, working paper, 15-03, août 2003, pp. 41 et 42 ; J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, *op. cit.*, p. 9 ; V. Papakonstantinou, *op. cit.,* p. 47 ; Projet de loi relatif à certains traitements de données à caractère personnel par le Service Public fédéral Finance, *Doc. Parl.,* Ch. Repr., sess. 2006-2007, n° 51 3064/001, pp. 73-74.

[161] « OASIS » est l'abréviation des termes « Organisation Anti-fraude des Services d'Inspection Sociale ».

Ce système, opérationnel depuis 2005[162], permet de mieux cibler et coordonner la lutte contre la fraude sociale de manière à mettre fin aux dégâts causés par ce type de fraude qui « mine le système de la sécurité sociale, organise une concurrence déloyale entre les entreprises et une discrimination inacceptable entre les personnes placées dans des conditions identiques »[163].

Cet entrepôt de données et les opérations qu'il rend possibles ne sont prévus par aucun texte légal ou réglementaire. Seules certaines décisions du Comité sectoriel de la sécurité sociale et de la santé, section sécurité sociale[164], balisent le fonctionnement de cette banque de données[165].

Après l'analyse du contenu de l'entrepôt de données OASIS, le profilage en matière sociale est étudié.

44.- OASIS. OASIS est un entrepôt de données.

Un entrepôt de données, plus couramment désigné sous le vocable anglais de « datawarehouse », est une banque de données d'un type particulier, qui se caractérise, principalement, par le fait qu'il contient un nombre considérable d'informations, organisées suivant une certaine logique devant permettre d'effectuer des recherches complexes à partir de celles-ci[166]. Les données enregistrées dans cet entrepôt sont choisies en fonction du but recherché par l'auteur de l'opération de profilage. Elles émanent d'une seule base de données ou de bases de données distinctes, c'est-à-dire initialement créées pour accomplir des

---

[162] Compte-rendu analytique de la Commission des Affaires sociales, *Doc. Parl.,* Ch. Repr., sess 2004-2005, COM 541, p. 19.

[163] Note de politique générale de la vice-première ministre et ministre de l'Emploi et de l'Egalité des chances du 15 avril 2008, *Doc. Parl.,* Ch. Repr., sess. 2007-2008, n° 52 0995/017, p. 61.

[164] Ci-après, ce Comité sectoriel est désigné par les termes « Comité sectoriel de la sécurité sociale ».

[165] Délibération n° 01/06 du 6 mars 2001 relative à une demande du Ministère fédéral des Affaires sociales, de la santé publique et de l'environnement pour la création et la gestion d'une banque de données OASIS en vue de la lutte contre la fraude sociale dans les secteurs de la construction, de la construction métallique, de l'électricité et des parcs et jardins ; Délibération n° 05/001 du 18 janvier 2005 relative à la création et gestion de la banque de données OASIS en vue de la lutte contre la fraude sociale – Délibération n° 01/06 du 6 mars 2001 – Extension de l'autorisation ; Délibération n° 06/079 du 17 octobre 2006 relative à l'échange de données entre la banque de données OASIS et la banque de données GENESIS.

[166] Pour de plus amples détails sur les caractéristiques d'un entrepôt de données, voy. N. Lefever et Y. Poullet, « Entrepôts de données et vie privée », *R.D.T.I.,* 2008, pp. 9 et 10 et les références citées à la note 3 de cet article ; C. Mues, « Datawarehouse 'Contrôles des transports routiers' (Politique scientifique fédérale – Agora/01/082) Rapport final et explication du projet de modèle », février 2004, pp. 5-12 disponible sur le site http://www.belspo.be/belspo/home/publ/pub_ostc/agora/ragff082_fr.pdf ; V. Papakonstantinou, *op. cit.,* pp. 46-49.

finalités différentes[167]. Une fois sélectionnées, ces informations peuvent être enregistrées dans l'entrepôt de données de plusieurs manières, sous forme de données nominatives, de données codées, ou encore sous forme de données anonymes[168].

OASIS contient des données relatives aux employeurs et aux travailleurs[169] de certains secteurs d'activité[170]. Elles sont issues d'une part, des sources authentiques de données sociales détenues par l'ONSS, l'ONEm et le SPF Finances[171] et, d'autre part, du cadastre des investigations[172]. À défaut d'avoir été prévue par un texte légal ou réglementaire, la liste des

---

[167] J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, *op. cit.*, p. 7 ; V. Papakonstantinou, *op. cit.,* p. 46.

[168] J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, *op. cit.*, p. 7.

[169] Selon le Comité sectoriel de la sécurité sociale, les données relatives aux travailleurs sont enregistrées dans OASIS « afin d'offrir aux inspecteurs sociaux une meilleure vue d'ensemble des employeurs » [Comité sectoriel de la sécurité sociale, délibération n° 05/001, *op. cit.,* p. 4].

[170] Il s'agit, pour l'heure, des secteurs de la construction, de la construction métallique, de l'électricité et des parcs et jardins [Délibération n° 01/06, *op. cit.,* p. 1], ainsi que, depuis 2005, des secteurs des grandes entreprises, des secteurs dans le prolongement du secteur de la construction, ainsi que certaines catégories de l'horeca de l'agriculture et de l'horticulture, du transport, de la confection et du nettoyage industriel [Délibération n° 05/001, *op. cit.,* p. 4].

[171] Ainsi, l'*ONSS* envoie des données provenant du répertoire des employeurs (qui contient, notamment, le code d'identification de l'employeur et son numéro de TVA), de la banque de données DMFA (qui signifie « déclaration multifonctionnelle ». Cette base de données contient, notamment, le montant des salaires payés aux travailleurs, le nombres d'heures prestées par ceux-ci, leur qualité d'employé, d'ouvrier ou d'apprenti), de la base de données DIMONA (qui contient, notamment, les déclarations d'emploi), du fichier 'chantiers et sous-traitants' (qui contient les déclarations préalables de chantiers qui doivent être introduites dans certaines hypothèses), du fichier 'entrepreneurs en règle', du fichier 'comptes et recouvrements' (qui contient, notamment, le relevé des créances de l'ONSS).

L'*ONEm* envoie des données provenant du fichier des procès-verbaux des inspecteurs sociaux du Ministère des Affaires sociales, de la Santé publique et de l'Environnement et du fichier 'chômeurs'.

Le *SPF Finances* envoie des données provenant du listing clients-fournisseurs à la TVA et du fichier des déclarations trimestrielles à la TVA. [voy. Comité sectoriel de la sécurité sociale, Délibération n° 01/06, *op. cit.,* p. 1, note 1 ; CPVP, Recommandation n° 01/2012 du 18 janvier 2012 concernant la possibilité d'un inventaire des banques de données pertinentes et d'une amélioration de l'échange d'informations dans le cadre de la lutte contre la fraude sociale, pp. 5 et 6 ; L.-A. Taufler, « The Datawarehouse OASIS », 1er février 2008, disponible sur le site http://litpc45.ulb.ac.be/OasisWorkshop/traufler.pdf ; entretien avec un fonctionnaire de l'Administration fédérale, le 17 juin 2008].

[172] Le cadastre des investigations est une source authentique de données provenant d'investigations menées par les services d'inspection sociale, créée et détenue par les services d'inspection de l'ONSS, de l'ONEm, du SPF Sécurité sociale et du SPF Emploi, Travail et Concertation sociale. Ces services d'inspection y introduisent des informations générales concernant les employeurs et relatives aux investigations réalisées à leur égard. Depuis

données communiquées à OASIS a été dressée par des informaticiens en fonction des besoins formulés par les inspecteurs sociaux[173]. L'autorisation du Comité sectoriel de la sécurité sociale a, en outre, été requise pour l'enregistrement des données relatives aux travailleurs[174].

Au total, 120 types de données ont initialement été enregistrés dans OASIS, auxquels 80 autres ont été ajoutés en 2006[175]. Ces données sont toutes enregistrées avec leur historique recouvrant une période de cinq ans[176].

> Par exemple, depuis le 6 mars 2001[177], l'ONSS est autorisée à communiquer à OASIS, entre autres informations nombreuses, des données issues notamment de la banque de données DMFA[178] et relatives aux employeurs et aux travailleurs exerçant leur activité notamment dans le secteur de la construction.
>
> En ce qui concerne les employeurs, il s'agit, par exemple, de leur numéro d'inscription à l'ONSS, du nombre de leurs employés et ouvriers, du nombre de jours rémunérés calculés sur la base des effectifs de personnel etc.
>
> Quant aux travailleurs, il s'agit, entre autres données, de leur NISS, de la rémunération trimestrielle brute à 100 %, du nombre de jours rémunérés, du nombre de jours de vacances etc. Par ailleurs, depuis le 18 janvier 2005[179],

quelques années, on enregistre dans OASIS une information issue de cette base de données, à savoir, le fait que l'employeur a déjà fait l'objet d'une investigation avec ou sans suite favorable [délibération 06/079, *op. cit.,* p. 3, pt 1.3].

[173] Entretien avec un fonctionnaire d'une administration fédérale, le 2 juin 2008. Après de nombreuses recherches, nous nous sommes tournés vers cette administration pour connaître avec exactitude les bases de données sociales à la source d'OASIS, ainsi que la liste des types de données communiqués à OASIS. Le 11 juin 2008, il nous a été répondu que ces précisions figuraient dans un dossier confidentiel, jadis confié au Comité sectoriel de la sécurité sociale pour rendre les autorisations susmentionnées, mais auquel nous ne pouvons avoir accès.

[174] Celles-ci sont issues des bases de données DMFA et DIMONA ainsi que du fichier des chômeurs de l'ONEm. Remarquons que le Comité sectoriel de la sécurité sociale considère que les seules données à caractère personnel dont il y a lieu d'autoriser la communication sont les informations relatives aux travailleurs. Pourtant, les informations relatives aux employeurs-personnes physiques sont également des données à caractère personnel au sens de la loi du 8 décembre 1992. Le Comité sectoriel et les administrations concernées refusent toutefois de l'admettre au motif que les informations relatives aux employeurs concernent son travail et non son intimité personnelle… [Entretien avec un fonctionnaire d'une administration fédérale le 17 juin 2008].

[175] Entretien avec un fonctionnaire d'une administration fédérale, le 4 juin 2008.

[176] Délibération n° 01/06, *op. cit.,* p. 1.

[177] Comité sectoriel de la sécurité sociale, Délibération n° 01/06, *op. cit.,* pp. 1 et s.

[178] DMFA est l'abréviation de « déclaration multifonctionnelle ». Il s'agit d'une source authentique de données détenue par l'ONSS et contenant les données de salaire et de temps de travail relatives aux travailleurs et qui ont été communiquées par l'employeur de ceux-ci.

[179] Comité sectoriel de la sécurité sociale, Délibération n° 05/001, *op. cit.,* pp. 1 et s.

> l'ONEm est autorisé à communiquer à OASIS des données relatives au chômage temporaire, telles que les dates de début et de fin du chômage, le NISS des travailleurs concernés, le numéro ONSS du chantier de construction, etc.

Les informations relatives aux employeurs, qu'ils soient une personne physique ou une personne morale, sont enregistrées telles quelles dans cet entrepôt de données. Par contre, les données relatives aux travailleurs font l'objet d'un codage, préalablement à leur enregistrement dans OASIS[180].

Concrètement, le codage des données des travailleurs consiste à coder le NISS de chaque travailleur selon la technique du hachage. En d'autres termes, le NISS est transformé en une chaîne de quarante caractères hexadécimaux, qui comprend des chiffres compris entre 0 et 9 et des lettres comprises entre A et F, tel que 3981d4f03f2732e582f629ba27af75a213cfc7f3. Ce faisant, il est impossible, à la seule lecture du NISS codé, de savoir à qui appartiennent les informations relatives à ce code. Ce codage est réalisé exclusivement par la Banque-Carrefour de la sécurité sociale qui gère une table de conversion reprenant, pour chaque code, le NISS auquel il correspond[181].

Afin de garantir la mise à jour des informations enregistrées initialement dans OASIS, les informations créées ou modifiées dans les sources authentiques de données sociales sont communiquées à OASIS selon une certaine fréquence qui dépend de la vitesse d'évolution de chacune de ces informations et conformément aux autorisations du Comité sectoriel de la sécurité sociale[182].

45.- La détection des scénarios de fraude et leur application en pratique. Avant l'utilisation du profilage, les personnes suspectées de fraude sociale étaient identifiées par les inspecteurs sociaux en fonction de leurs connaissances en matière de fraude sociale. Ceux-ci décrivaient aux informaticiens le type de fraudeur recherché afin qu'ils établissent certains rapports informatiques entre les fichiers détenus par les administrations concernées.

Cette méthode souffrait du fait qu'à un moment donné, les inspecteurs sociaux avaient livré toutes leurs connaissances sans que, pour

[180] Remarquons que, comme l'a rappelé le Comité sectoriel de la sécurité sociale, des données codées sont des données à caractère personnel, étant donné que les personnes qu'elles concernent sont indirectement identifiable « notamment par le biais de la table de conversion gérée par la Banque-Carrefour » [Délibération n° 01/06, *op. cit.,* p. 2].

[181] Délibération n° 01/06, *op. cit.,* p. 8.

[182] Entretien avec un fonctionnaire d'une administration fédérale, le 11 juin 2008.

autant, on ait découvert toutes les fraudes. En outre, les inspecteurs sociaux pouvaient de moins en moins compter sur les plaintes des travailleurs pour aiguiller leurs recherches[183]. En effet, suite à une modification législative, les travailleurs à mi-temps ont obtenu le droit d'avoir la même couverture sociale que les travailleurs à temps plein, c'est-à-dire une couverture complète. Cela a généré des fraudes nouvelles difficilement détectables, car des employeurs se sont mis à déclarer des travailleurs à mi-temps, alors qu'en pratique, ces derniers effectuaient un travail à temps plein. Cela permettait aux premiers de payer moins de charges sociales tandis que les seconds, bénéficiant des mêmes droits de la sécurité sociale, ne portaient pas plainte à l'ONSS. Il devenait donc nécessaire de trouver un outil permettant aux inspecteurs sociaux de cibler leurs recherches sans compter sur les indications fournies par les travailleurs.

Aujourd'hui, ces limites sont dépassées grâce aux puissants calculs effectués à partir d'OASIS, qui permettent d'identifier davantage de fraudeurs potentiels. Ainsi, on applique aux données enregistrées dans OASIS un certain nombre d'alarmes, qui sont des algorithmes de détection de fraude mettant en relation quelques données déterminées. Si une alarme se déclenche au sujet d'un employeur, cela signifie que celui-ci est suspect au regard du type de fraude traité par l'alarme.

> Par exemple, l'alarme 16*bis* détecte la « présence d'une valeur ajoutée élevée sans paiement de cotisations ONSS ». En d'autres termes, cette alarme identifie comme fraudeurs potentiels les employeurs dont l'entreprise présente une augmentation moyenne du chiffre d'affaire de 20 % minimum alors qu'il n'y a que peu de personnel déclaré.
>
> Pour ce faire, l'alarme met en relation le matricule de l'employeur, qui est une donnée d'OASIS provenant du répertoire des employeurs, les déclarations TVA, provenant du SPF Finances, et le nombre de jours de travail rémunérés, provenant du fichier DIMONA.
>
> Le calcul appliqué est le suivant : si ((CA1/CA0)[184] -1)> P1 et JR=6 alors l'alarme s'enclenche. En d'autres termes, si l'augmentation du chiffre d'affaire formulé par ((CA1/CA0)-1) est supérieur à 20 % (>P1) et que le nombre de jours rémunérés (JR) est égal à 6, alors, l'employeur concerné est identifié comme un fraudeur potentiel.

[183] *Idem.*

[184] Le chiffre d'affaire est calculé sur quatre trimestres, pour éviter que les employeurs ne prétendent qu'ils ont englobé les frais d'un trimestre dans la comptabilité du trimestre suivant. Ainsi, CA1 est le chiffre d'affaire pour le trimestre t et résulte du calcul suivant : (t + t-1 + t-3) /3, tandis que CA0 est le chiffre d'affaire pour le trimestre t-1 qui est le résultat du calcul suivant : (t + t-1 + t-3) / 3.

Néanmoins, en pratique, l'enclenchement d'une seule alarme ne suffit pas pour engager une inspection sociale auprès de l'employeur. C'est pourquoi, lors de la détection de fraude via OASIS, on conjugue plusieurs alarmes choisies à partir de profils de types de fraudeurs[185]. En d'autres termes, on met en concordance plusieurs alarmes en partant de l'idée que, si un certain type de fraude est commis, il y a fort à parier qu'un autre type de fraude est également réalisé.

> Par exemple, au sein d'OASIS, on conjugue notamment les alarmes 3 et 4*ter*.
>
> L'alarme 3 détecte les entreprises dans lesquelles il y a une forte augmentation du personnel sur une courte période de temps. Elle est conjuguée avec l'alarme 4*ter* qui met en évidence une proportion importante de dettes à l'ONSS.

Cette conjugaison d'alarmes répond au profil-type des entreprises de pourvoyeurs de main-d'œuvre, c'est-à-dire des entreprises qui engagent beaucoup de personnel, déclarent chaque travailleur mais ne paient pas à l'ONSS les charges sociales relatives à ceux-ci. Le temps que l'ONSS s'en rende compte et décide de mener une inspection sociale, les travailleurs concernés sont déplacés – souvent en masse – dans une autre entreprise, qui recommence le même type de fraude. L'alarme 3 permet de détecter l'arrivée massive de ces travailleurs qui seront déclarés mais pour lesquels l'employeur ne paiera pas de charges sociales et l'alarme 4 permet de mettre en évidence qu'à partir de l'arrivée de ces travailleurs, des dettes sont nées à l'ONSS. Lorsque ces deux alarmes se déclenchent pour une même période et concernent un même employeur, les inspecteurs sociaux voient apparaître sur leur écran un tableau semblable à celui-ci[186] :

[185] B. Deroost, H. Meurisse, D. Renauld et K. Velle, « De missie en de doeltreffendheid van de controlediensten van de Federale Overheid. Casus : De inspectiedienst van de Dients Toelagen en Contrôle van de POD Maatschappelijke integratie. Adviesopdracht », disponible sur le site http://soc.kuleuven.be/io/pmpucl/advies/160126_adviesMI.pdf.

[186] Entretien avec un fonctionnaire de l'Administration fédérale, le 17 juin 2008. Le tableau est repris du document suivant : L.-A. Taufler, « The Datawarehouse OASIS », 1er février 2008, disponible sur le site http://litpc45.ulb.ac.be/OasisWorkshop/traufler.pdf.

Année :	2008	Région choisie :	Hainaut
Matricule choisi :		Sélection complète	

		Alarme BC 4 Ter				Alarme BC 3				
Matricule	Importance	Mois	% de croissance du solde courant/ solde moyen	Solde courant	Solde courant (mois précédent)	Pourcentage d'augmentation	Nombre travailleurs avant	Nombre travailleurs après	Signalé pour le mois	
132227101	20-49 tr	1	74,50	96.115,95	55.080,09	100,00	13	26	2007	4
132227101	20-49 tr	2	0,00	55.080,09	55.080,09	100,00	13	26	2007	4
132227101	20-49 tr	3	188,81	159.074,60	55.080,09	100,00	13	26	2007	4
132227101	20-49 tr	4	0,00	159.074,60	159.074,60	100,00	13	26	2007	4
132334480	10-19 tr	1	0,00	27.744,43	27.744,43	220,00	5	16	2007	4
132497537	5-9 tr	3	0,00	31.714,35	31.714,35	120,00	5	11	2007	8
132497537	5-9 tr	4	0,00	31.714,35	31.714,35	120,00	5	11	2007	8
132589202	1-4 tr	4	369,09	14.345,15	3.058,09	1.000,00	1	11	2007	10
132707348	5-9 tr	1	-67,27	12.363,51	37.779,23	85,71	7	13	2007	10
132707348	5-9 tr	2	-67,27	12.363,51	37.779,23	85,71	7	13	2007	10
132707348	5-9 tr	3	0,00	37.779,23	37.779,23	85,71	7	13	2007	10
132707348	5-9 tr	4	0,00	37.779,23	37.779,23	85,71	7	13	2007	10
132720637	20-49 tr	4	0,00	71.982,74	71.982,74	53,85	13	20	2007	8
132778837	10-19 tr	1	0,00	11.111,52	11.111,52	150,00	6	15	2007	9
132778837	10-19 tr	2	-69,95	11.785,82	39.223,31	150,00	6	15	2007	9
132778837	10-19 tr	3	0,00	39.223,31	39.223,31	150,00	6	15	2007	9
132778837	10-19 tr	4	0,00	39.223,31	39.223,31	150,00	6	15	2007	9

Sur ce tableau, on peut voir, par exemple, que l'employeur dont le matricule au répertoire des employeurs est 132227101 a engagé, en janvier 2007, treize travailleurs, et que sa dette auprès de l'ONSS, pour cette période, est passée de 55.080,09 euros à 96.115,95 euros, soit, une augmentation de la dette de 74 %.

Ce faisant, on peut, grâce à OASIS, mettre en évidence des employeurs qui sont des fraudeurs potentiels. Mais il ne s'agit là que d'un indicateur, qui ne peut dispenser les inspecteurs sociaux d'opérer des vérifications effectives sur le terrain. En effet, en pratique, il peut arriver que soient mis en évidence des employeurs qui ne sont pas, en réalité, des fraudeurs[187]. Pour reprendre l'exemple ci-dessus, ce n'est pas, en soi, une fraude d'engager treize travailleurs sur le même mois. Quant aux dettes à l'ONSS, si elles sont existantes pendant une certaine période identifiée par OASIS, elles peuvent avoir été régularisées au moment de l'inspection sociale.

Pour mener à bien une inspection sociale, il peut s'avérer nécessaire d'effectuer des recherches plus précises concernant certains travailleurs de l'entreprise, et non seulement leur employeur. Néanmoins, les travailleurs de l'entreprise suspectée de fraude ne peuvent être identifiés à partir des seules données enregistrées dans OASIS, puisque leur NISS y est codé. Il y a donc lieu de consulter la table de conversion détenue par la Banque-Carrefour de la sécurité sociale afin de décoder le NISS de ces personnes, après y avoir été autorisé par le Comité sectoriel de la sécurité sociale[188]. À partir des NISS décodés des travailleurs et de certaines données d'identification des employeurs, les inspecteurs sociaux peuvent effectuer des consultations ciblées dans les différentes banques de données sociales, à condition d'être autorisés par le Comité sectoriel de la sécurité sociale à consulter ces dernières[189].

---

[187] Entretien avec un fonctionnaire d'une administration fédérale, le 17 juin 2008.

[188] Délibération n° 01/06, *op. cit.,* p. 8. Ce Comité sectoriel a décidé que « les inspecteurs sociaux du Ministère des Affaires sociales, de la Santé publique et de l'Environnement, du Ministère de l'Emploi et du Travail, de l'ONSS et de l'ONEm, sont autorisés à consulter auprès de la Banque-Carrefour [...] la table de conversion [...]. La Banque-Carrefour fera périodiquement rapport au Comité de surveillance sur le nombre de consultations effectuées ».

[189] L'accès à la base de données DIMONA a été autorisé par le Comité de surveillance près la Banque-Carrefour de la sécurité sociale (qui assurait, jadis, les fonctions de l'actuel Comité sectoriel de la sécurité sociale) à l'Inspection sociale du Ministère des Affaires sociales, de la Santé publique et de l'Environnement (délibérations n° 95/47 du 12 septembre 1995 et n° 99/91 du 5 octobre 1999) et à l'Inspection des Lois Sociales du Ministère de l'Emploi et du Travail (délibérations n° 99/04 du 5 janvier 1999 et n° 00/25 du 1er février 2000) ; la communication de donnés sociales à caractère personnel par des institutions de sécurité sociale aux services d'inspection sociale a également été autorisée (délibération n° 98/63 du 13 octobre 1998) ; la consultation du cadastre des investigations a été autorisée par le Comité sectoriel de la sécurité sociale aux services d'inspection de l'ONSS, de l'ONEm, du SPF sécurité sociale et du SPF Emploi, Travail et Concertation sociale (délibération n° 04/44 du 7 décembre 2004) ; la consultation du Registre national des personnes physiques, de certains registres de la Banque Carrefour de la sécurité sociale, du registre d'attente, du registre des cartes SIS, de la banque de données DIMONA, du fichier du personnel des employeurs immatriculés à l'ONSS ou à l'ONSSAPL, du fichier DMFA, du répertoire des employeurs, du fichier de déclaration de travaux et du fichier GOTOT a été autorisée pour la

Par exemple, l'alarme 43 permet d'identifier les entreprises ayant déclaré un nombre de jours de chômage économique ou pour cause d'intempéries supérieur à la moyenne du secteur. En combinant cette alarme à l'alarme 45 bis qui indique le NISS codé des ouvriers de l'entreprise pour lesquels des jours de chômage sont enregistrés dans le fichier DMFA mais non à l'ONEm, on peut suspecter du travail au noir. Il est donc intéressant de décoder le NISS de ces ouvriers pour aller voir sur place si ces personnes ont effectivement travaillé pendant la période de chômage déclarée.

Section 2. Des craintes nouvelles

46.- Enthousiasme et prudence. Bien évidemment, le déploiement de l'e-gouvernement est enthousiasmant. Il offre d'indéniables avantages, tant en ce qui concerne l'efficacité de l'administration que l'égalité entre les citoyens. Ces avancées, techniques et sociales, justifient assurément que le développement de l'e-gouvernement soit encouragé.

L'e-gouvernement favorise l'*efficacité* de l'administration, parce que les échanges de données informatisés, l'enregistrement d'informations fiables dans les sources authentiques de données, les documents administratifs accessibles en ligne, les informations importantes mises sur le site internet des administrations, la possibilité de remplir sa déclaration fiscale sur internet, sont autant d'avancées technologiques qui permettent aux administrations et aux citoyens d'économiser du temps et de l'argent. Les agents des administrations se voient ainsi épargner l'exécution de tâches bureaucratiques pesantes. Ils peuvent se consacrer à d'autres missions. Cet argument a d'ailleurs été avancé lors de la mise en place de la Banque-Carrefour de la sécurité sociale, soutenant que « la suppression des redondances dans la collecte, l'enregistrement et le traitement des données sociales à caractère personnel, [...], l'organisation des relations administratives entre les institutions de sécurité sociale sur des bases nettement plus efficaces, [...] constituent autant d'éléments qui permettront de réaliser des économies au niveau des frais de fonctionnement administratif »[190]. Les citoyens bénéficient également d'un plus grand confort

Direction générale Contrôle des lois sociales du SPF Emploi, Travail et Concertation sociale, pour l'Inspection sociale du SPF Sécurité sociale, pour le service d'inspection de l'ONSS, pour le service d'inspection de l'ONSSAPL, pour le service d'inspection de l'ONEm et pour le service d'inspection du FAT (délibération n° 04/032 du 5 octobre 2004).

[190] Rapport fait au nom de la Commission des affaires sociales par Mme Nelis-Van Ledekerke, *Doc. Parl.,* Ch. Repr., 1988-1989, n° 899/4, repris dans *Pasin.,* I, 1990, p. 128.

dans leurs démarches administratives qu'ils peuvent effectuer en ligne. En outre, grâce à la collecte unique de données, ils ne doivent plus fournir la même information à de multiples occasions.

Par ailleurs, l'e-gouvernement œuvre également au respect de l'*égalité* entre les citoyens. Les outils informatiques qui permettent, par exemple, de retrouver plus rapidement les fraudeurs contribuent à assurer l'égalité devant l'impôt. Dans le même sens, l'automatisation des droits permet à chacun d'obtenir l'allocation à laquelle il peut prétendre. C'est particulièrement important pour les plus faibles qui sont bien souvent les premières victimes de la lourdeur bureaucratique car leur handicap ou l'absence de domicile fixe, par exemple, rend d'autant plus difficile l'attention qu'il faut porter aux échéances administratives et aux documents à remplir et à renvoyer à la personne compétente.

Néanmoins, ces avancées enthousiasmantes ne doivent pas être aveuglantes. La prudence est de mise. Sans nier les avantages offerts par l'e-gouvernement, il convient de prendre conscience du fait que l'informatisation de l'administration génère des craintes. Il y a lieu de les circonscrire au mieux, afin de ne pas leur laisser de place au moment d'organiser la structure et le fonctionnement de l'e-gouvernement. En somme, on peut dire que la mise en place de l'e-gouvernement doit allier « l'optimisme de la volonté »[191] – c'est-à-dire la confiance, l'énergie et les idées pour faire progresser le fonctionnement de l'administration – et « le pessimisme de l'intelligence »[192] – à savoir, la prise en compte lucide des dangers réels que recèle l'e-gouvernement. Dans le même sens, Jacques Chevallier affirme qu' « au-delà des perspectives séduisantes », il faut « faire preuve de prudence : ni optimisme béat, ni enthousiasme aveugle ; c'est peut-être le signe qu'on est parvenu à l'âge de la maturité »[193].

L'e-gouvernement génère de nombreuses craintes. En particulier, un important déséquilibre entre l'administration et les citoyens risque d'être créé. Dans le même temps, on redoute la normalisation des comportements des individus, le développement d'une technocratie, sans oublier les failles dans la sécurité informatique.

---

[191] Selon l'expression de Antonio GRAMSCI, dans une Lettre à son frère Carlo écrite en prison, le 19 décembre 1929 (*Cahiers de prison* 1, 2, 3, 4 et 5, Paris, Gallimard, 1996).

[192] *Idem*.

[193] J. CHEVALLIER, « La mise en œuvre de l'administration électronique », *in* L'administration électronique au service des citoyens. Actes du colloque organisé par le Conseil d'État et l'Université Paris I Panthéon Sorbonne à Paris, les 21 et 22 janvier 2002 (dir. G. CHATILLON et B. DE MARAIS), Bruxelles, Bruylant, 2003, p. 388.

I. Un déséquilibre important entre l'administration et les citoyens

47.- La prise du citoyen sur l'administration. Dans notre société démocratique, on veille à ce que le citoyen puisse exercer une certaine prise sur l'administration, pour la comprendre, la contrôler voire la contester.

Ce souci a émergé en réaction à l'organisation archaïque de l'administration de jadis, distante, imposant unilatéralement ses commandements à des citoyens soumis et méfiants. L'administration se conçoit désormais non comme une « tyrannie monolithique mais comme une communauté intégrée »[194], qui « réclame qu'une place structurelle soit accordée aux garanties constitutionnelles de liberté de parole, d'association et de religion, toutes ces libertés qui sont nécessaires pour permettre et encourager les individus à prendre leurs responsabilités au nom de leurs convictions personnelles »[195]. Ce souci justifie d'ailleurs nombre de développements du droit administratif. Comme le remarque David De Roy, « au cours des dernières décennies, les relations entre l'administration et le citoyen ont évolué dans un sens résolument favorable à ce dernier, évolution dont rendent compte les obligations de transparence et de motivation qui incombent à l'administration, ainsi que l'accroissement considérable des ressources de la protection juridictionnelle à l'égard de l'arbitraire administratif »[196].

La relation entre l'administration et le citoyen est aujourd'hui ébranlée par l'utilisation des technologies dans l'administration, comme on le constate au travers des exigences de légalité, de transparence et de contrôle applicables à l'administration[197].

---

[194] M. Verdussen, « La signification du principe de l'État de droit pour l'administration en Europe », *in Verfassungsprinzipien in Europa, Constitutional principles in Europa – Principes constitutionnels en Europe*, (H. Bauer et C. Callies éd.), Athènes, Berlin, Bruxelles, Ant. N. Sakkoulas, Berliner wissenschaft-verlag, Bruylant, 2008, p. 193.

[195] R. Dworkin, « Deux conceptions de la démocratie », *in L'Europe au soir du siècle. Identité et démocratie* (dir. J. Lenoble et N. Dewandre), Paris, Esprit, 1992, p. 134. Voy. égal. du même auteur, « Equality, Democracy, and Constitution : We the People in Court », *Alberta Law Review,* 1990, vol. 28, p. 341.

[196] D. De Roy, « La nature des prétentions de l'usager au bénéfice des prestations de service public : essai de typologie », *in Le service public : passé, présent et avenir* (dir. H. Dumont, P. Jadoul, B. Lombaert, F. Tulkens, S. Van Drooghenbroeck), T. 1, Bruxelles, La Charte, 2009, p. 483.

[197] Comme on l'a dit dans l'introduction de la thèse, et comme nous le détaillerons encore par la suite, parmi les exigences qui s'imposent à l'administration, les exigences de légalité, de transparence et de contrôle retiennent notre attention et font l'objet d'amples développements dans la suite de cette recherche. Néanmoins, pour la compréhension des lignes qui

48.- Dans l' « administration papier ». Dans l'administration traditionnelle, que l'on nomme « administration papier » pour désigner l'administration non encore informatisée, les exigences de légalité, de transparence et de contrôle permettent au citoyen d'exercer une certaine prise sur l'administration.

Certes, l'administration détient des informations sur chaque citoyen, liées à l'exercice de ses missions. Mais, en face d'elle, le citoyen dispose de voies juridiques permettant d'entrer en contact avec elle, de forcer le dialogue. Ces moyens d'action permettent en principe à tout individu de comprendre l'action administrative et, le cas échéant, de réagir aux illégalités. L'État et le citoyen exercent donc une certaine prise l'un sur l'autre.

Ainsi, l'exigence de légalité veut qu'en lisant la loi, tout individu soit à même de percevoir les missions dévolues aux pouvoirs publics et de vérifier que ces derniers n'outrepassent pas leurs compétences. Elle doit également garantir au citoyen que les balises qui entourent l'administration ont été discutées par les élus de la Nation.

En vertu de l'exigence de transparence, toute personne peut accéder aux documents administratifs, comprendre les éléments sur lesquels l'administration a fondé une décision et corriger les éventuelles inexactitudes affectant les informations utilisées.

La volonté d'instaurer un dialogue entre l'administration et le citoyen est d'ailleurs particulièrement flagrante s'agissant de l'importance qu'a prise l'exigence de transparence de l'administration. Comme nous le détaillerons dans le Titre II de cette recherche qui aborde la transparence administrative, l'exposé des motifs de la loi du 11 avril 1994, notamment, confirment ces propos. Ainsi, le Ministre de l'Intérieur de la Fonction publique a-t-il soutenu que « dans toute organisation politique, le citoyen doit occuper une position centrale et on ne peut accorder à aucune structure le droit ni le pouvoir de se substituer au citoyen, ni de le mettre dans une position d'inégalité et, par hypothèse, d'infériorité. Il va sans dire qu'un tel principe doit également s'appliquer à l'administration, à son organisation et à son fonctionnement »[198].

Par ailleurs, puisque l'administration est contrôlée par des instances juridictionnelles, un individu peut notamment obtenir l'annulation d'un acte administratif illégal ou la condamnation de l'administration à réparer le dommage causé par sa faute.

---

suivent, nous les mentionnons très brièvement ici. L'exigence de *légalité* impose que l'action administrative soit encadrée clairement par le législateur. L'exigence de *transparence* organise la mise en lumière de l'action administrative. L'exigence de *contrôle* aboutit à ce que les illégalités commises dans l'administration soient sanctionnées par le cours et tribunaux.

[198] Projet de loi relatif à la publicité de l'administration, Exposé des motifs, *op. cit.*, p. 4.

49.- Dans l'e-gouvernement. L'administration informatisée est considérablement plus puissante que l'administration papier, si bien que les moyens dont dispose actuellement le citoyen ne suffisent plus pour comprendre et contrôler l'action administrative[199].

a) Des moyens techniques puissants pour l'administration. Ce gain de puissance de l'administration s'explique principalement par le fait que l'administration détient toujours plus d'informations au sujet des individus, et qu'elle peut les exploiter davantage[200]. Concrètement, « there is virtually no limit to the amount of information that can be recorded, b) there is virtually no limit to the scope of analysis that can be done – bounded only by human ingenuity, and c) the information may be stored virtually forever »[201].

Les pouvoirs publics recueillent et enregistrent aujourd'hui un grand nombre d'informations sur chaque citoyen, qui touchent à tous les aspects de leur vie. Initialement, cette accumulation de données s'explique par le fonctionnement de l'État providence : puisque l'État doit fournir de nombreuses prestations à la population, il doit connaître les singularités de chaque citoyen. Ces derniers y consentent, puisqu'ils désirent bénéficier des droits sociaux qui leur reviennent.

---

[199] En ce sens, S. Gutwirth, « De toepassing van het finaliteitsbeginsel », *T.P.R.,* 1993, II, pp. 1424 à 1428 ; Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in État de droit et virtualité* (Éd. K. Benyekhlef et P. Trudel), Montréal, Thémis, 2009, p. 207. Ces derniers soutiennent que cette « asymétrie de pouvoir » explique l'élaboration du régime de protection des données. Nous revenons sur ce point dans le chapitre suivant.

[200] En ce sens, H. P. Gassman et G. R. Pipe, « Rapport de synthèse », *in OCDE. Études d'informatique. 10 questions d'ordre politique soulevées par la protection des données et des libertés individuelles. Principes et perspectives. Compte rendu du séminaire 24-26 juin 1974*, Paris, OCDE, 1976, p. 13 ; A. Roux, *La protection de la vie privée dans les rapports entre l'État et les particuliers*, Paris, Economia, 1983, p. 140 ; M. R. V. Jones, « La vie privée mise en péril par la technologie », *in Vie privée et droits de l'homme, Actes du 3e colloque international pour la Convention européenne des droits de l'homme (Bruxelles 30 septembre-30 octobre 1970)*, Bruxelles, Bruylant, 1973, p. 209 ; H. Maisl, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », *in L'administration électronique au service des citoyens* (dir. G. Chatillon et B. du Marais), *op. cit.*, p. 350 ; R. Leenes et B.-J. Koops, « 'Code' and privacy or how technology is slowly eroding privacy' », *in Coding regulation. Essays on the Normative Role of Information technology* (dir. E. Dommering et L. Asscher), La Haye, TMC Asser Press, 2006, pp. 177 et 178 ; J. Ringelheim, « Recueil de données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », *in De nieuwe federale antidiscriminatiewetten – Les nouvelles lois luttant contre la discrimination* (C. Bayart, S. Sottiaux et S. Van Drooghenbroeck éd.), Brugge, Bruxelles, die Keure, La Charte, 2008, p. 81.

[201] H. Nissenbaum, « Protecting Privacy in a Information Age : the Problem of Privacy in Public », *Law and Philosophy,* 1998, vol. 17, p. 576.

Par la suite, les outils informatiques ont facilité et donc encouragé la collecte et la mémorisation de ces innombrables informations. Nul besoin d'envoyer plusieurs formulaires en papier ni d'organiser le classement de ceux-ci dans d'imposantes armoires. Les technologies offrent un gain de temps, et d'espace, ce qui rend d'autant plus tentantes la collecte d'informations et la multiplication des bases de données.

En outre, grâce aux technologies, les pouvoirs publics peuvent exploiter ces nombreuses informations de manière plus fine que jadis, ce qui augmente notamment leur capacité de contrôle des citoyens. En effet, la circulation des données est plus aisée et plus rapide. Techniquement, on peut, en quelques « clics », regrouper les informations relatives à un individu, même si elles sont disséminées dans diverses administrations.

> Par exemple, la commune de Namur pourrait être tentée de demander à la Région wallonne les informations que celle-ci détient au sujet de l'habitation de John, et qu'elle a collectées dans le cadre de sa mission d'inspection du logement (données relatives aux exigences de sécurité et de salubrité notamment). La commune pourrait alors confronter ces données au permis de bâtir que John a introduit jadis à la commune, dans le but de sanctionner les infractions urbanistiques et réviser le revenu cadastral[202].

Ce regroupement d'informations est rendu possible parce que de nombreuses administrations utilisent le numéro d'identification au Registre national, pour identifier de manière unique chaque citoyen dans leurs fichiers. Par exemple, l'intégrateur de services fédéral, qui coordonne les échanges électroniques de données entre toutes les autorités fédérales, utilise le numéro d'identification au Registre national[203]. Ce même numéro d'identification est également utilisé par la Banque-Carrefour de la sécurité sociale[204], et par l'administration fiscale[205]. Au final, le numéro d'identification du Registre national est utilisé dans des réseaux sectoriels qui sont non seulement très étendus, mais au sein desquelles on peut aller puiser des informations qu'on regroupe et rattache à l'individu concerné, vu l'utilisation d'un même numéro d'identification. On peut donc obtenir toutes les informations relatives au citoyen concerné – telles que ses données médicales, le montant de ses revenus, sa situation patrimoniale,

[202] Cette hypothèse a fait l'objet de l'avis de la CPVP n° 18/2008 du 30 avril 2008 demandé par la Région de Bruxelles-Capitale, Administration de l'Aménagement du Territoire et du Logement, Direction de l'Inspection régionale du Logement relatif à la communication à une administration communale de données recueillies en application du Code bruxellois du Logement.

[203] Art. 5 de la loi sur l'intégrateur de services fédéral précitée.

[204] Art. 7 de la loi sur la Banque-Carrefour de la sécurité sociale précitée.

[205] Art. 314, §1, al. 1 et 2, C.I.R 92.

la composition de sa famille, etc. – même si elles se trouvent dans des bases de données disséminées dans des administrations distinctes.

Dans l'administration papier, une telle concentration d'informations était sans doute trop complexe pour que l'on soit tenté de l'effectuer. En effet, chaque administration transcrivait les informations dont elle avait besoin sur des fiches en papier. Celles-ci étaient classées dans des armoires. Dans ce contexte, pour obtenir une information relative à un citoyen, il fallait s'adresser à l'administration susceptible de disposer de l'information recherchée, au sein de laquelle il fallait identifier la personne compétente. Celle-ci devait ensuite trouver la bonne information dans la bonne armoire et le bon fichier, en espérant qu'il n'y ait pas de confusion entre deux citoyens portant le même nom. Elle devait enfin photocopier la fiche, la mettre sous enveloppe timbrée et porter l'enveloppe à la Poste. Une telle procédure est si fastidieuse qu'on n'était probablement pas tenté de la réaliser[206].

Plus encore, la technique du profilage utilisée par l'administration[207] permet de classer les personnes concernées dans une catégorie prédéterminée de la population. Celles-ci se voient alors attribuer, à titre personnel, les caractéristiques comportementales de ce groupe. Elles seront ensuite soumises à l'attitude que l'administration réserve à cette catégorie de la population et qui peut s'apparenter à de la méfiance voire de l'hostilité si, par exemple, la personne est rattachée à la catégorie des fraudeurs fiscaux. Un tel jugement prospectif risque de paraître d'autant plus crédible qu'il est le résultat d'une opération effectuée par la voie informatique, réputée neutre et infaillible[208].

---

[206] Dans le même sens, A. VITALIS, *Informatique, Pouvoir et Libertés,* 2e éd., Paris, Economica, 1988, pp. 84, 88 et 147 ; A. TOUFFAIT, « Libertés publiques et Informatique », *Gazette du Palais,* 9 août 1973, p. 3 ; A. ROUX, *La protection de la vie privée dans les rapports entre l'État et les particuliers, op. cit.,* pp. 74-75 ; S. RODOTA, « Protection de la vie privée et contrôle de l'information : deux sujets d'inquiétude croissante pour l'opinion publique », *in OCDE. Études d'informatique. 10 questions d'ordre politique soulevées par la protection des données et des libertés individuelles. Principes et perspectives. Compte rendu du séminaire 24-26 juin 1974, op. cit.,* p. 161 ; K.S. SELMER, « Normes à observer pour le traitement de l'information et les processus de contrôle », *in OCDE. Études d'informatique. 10 questions d'ordre politique soulevées par la protection des données et des libertés individuelles. Principes et perspectives. Compte rendu du séminaire 24-26 juin 1974, op. cit.,* p. 88 qui affirme que « cette répartition de l'administration de l'État tout entier en branche séparées constitue le moyen le plus efficace de protection de la 'vie privée' ».

[207] Voy. *supra,* nos 40.- et s.

[208] F. RIGAUX, « La protection de la vie privée à l'égard des données à caractère personnel », *Ann. Dr. Louvain,* 1993, T. III, pp. 64-65 ; F. RINGELHEIM, « Vie privée et protection des données sociales », *Rev. Dr. Soc.,* 1994, p. 300 ; D. SOLOVE, « I've got nothing to hide' and other misunderstandings of privacy », *San Diego Law Review,* 2007, vol. 44,

> On a mentionné préalablement l'entrepôt de données OASIS, qui regroupe de multiples informations relatives aux entrepreneurs, notamment, et les confronte au profil de fraudeur social. Si l'alarme est enclenchée, cela signifie que cet individu est vraisemblablement un fraudeur et qu'une inspection sociale doit être menée auprès de lui.

b) Des moyens juridiques insuffisants pour le citoyen. Les voies juridiques traditionnelles permettant d'assurer la légalité, la transparence et le contrôle de l'administration ne suffisent plus pour permettre au citoyen de garder une prise sur l'action de l'administration.

La légalité de l'action administrative est ainsi ébranlée, car nombre de ces évolutions technologiques ne sont pas encadrées par la loi[209]. Elles n'ont donc pas bénéficié d'un débat démocratique et ne sont pas définies dans une norme légale. L'encadrement de l'e-gouvernement paraît donc très obscur.

L'e-gouvernement manque également de transparence dans son fonctionnement. Pour de multiples raisons que nous développerons ultérieurement[210], il est en effet difficile, pour tout un chacun, de savoir ce que l'administration détient sur lui, ce qu'elle fait de ses données, comment fonctionnent les outils de traitement de données, etc.

Enfin, les recours juridiques à disposition du citoyen semblent également mal adaptés au contrôle de l'e-gouvernement, notamment en raison du fait que leur lourdeur contraste avec la rapidité des développements technologiques[211].

On se trouve dès lors confronté à une situation dans laquelle le citoyen est transparent aux yeux de l'administration puisque celle-ci peut aisément se faire une idée très précise de chaque personne, à partir des nombreuses données qu'elle détient à leur sujet. En revanche, l'administration peut œuvrer dans une grande opacité, compte tenu du peu de prise que le citoyen a encore sur son action[212]. Il est d'ailleurs paradoxal que les outils informatique mis en place, qui doivent notamment faciliter l'accès des citoyens à l'administration et leur contact avec elle, aboutissent à masquer la logique des décisions prises. On peut ainsi affirmer que « le système

---

p. 766 ; A. Roux, *La protection de la vie privée dans les rapports entre l'État et les particuliers, op. cit.,* pp. 74-75 ; D. Kaplan, *Informatique, libertés, identités,* Paris, Éd. FYP, 2010, p. 34 ; M. Hildebrandt, *op. cit.,* pp. 242 à 244.

209 À ce sujet, voy. Titre I.

210 Voy. Titre II.

211 Voy. Titre III.

212 À ce sujet voy. P. De Hert et S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", *in Privacy and the Criminal Law,* (dir. E. Claes, A. Duff et S. Gutwirth), Anvers, Oxford, Intersentia, 2006, pp. 61 à 104.

même chargé de clarifier l'information devient de plus en plus opaque pour la plupart des utilisateurs [...] Cela met en évidence un processus qui a des conséquences importantes pour la démocratie »[213]. Dans ce contexte, on ne peut plus soutenir que le citoyen dispose encore de prises suffisantes sur l'administration si bien qu'un déséquilibre important caractérise la relation entre l'administration et le citoyen dans l'e-gouvernement.

Pour illustrer cette problématique, les risques engendrés par le profilage sont particulièrement éloquents. L'attribution d'un profil à une personne déterminée permet « de générer des nouvelles données à caractère personnel qui ne sont pas celles que la personne concernée a communiquées au responsable de traitement ou dont elle peut raisonnablement présumer la connaissance par le responsable de traitement »[214]. Or, d'une part, ces nouvelles données sont peut-être inexactes. Pourtant, le citoyen n'est pas en mesure de corriger les éventuelles erreurs. Le profilage peut alors aboutir à imposer aux individus des décisions plus ou moins graves, telles qu'un contrôle fiscal ou le refus d'accéder à un emploi, alors que ces décisions sont prises sur la base d'éléments dont la véracité n'est pas nécessairement avérée. Certaines personnes seront donc affectées par une décision injuste à leur égard, car dénuée de tout fondement[215]. D'autre part, le profilage se fait souvent dans l'ombre ou est peu compris des citoyens vu sa complexité. Il est donc particulièrement difficile pour la personne concernée de vérifier les opérations effectuées et de comprendre les décisions qui en découlent.

Le droit à la protection des données à caractère personnel, qui s'enracine dans le droit à la protection de la vie privée, a été conçu pour pallier de tels risques. Nous y reviendrons dans le chapitre suivant[216].

II. La normalisation des comportements

50.- Une incitation au conformisme. On vient de pointer l'opacité qui entoure l'e-gouvernement, en constatant qu'il est actuellement difficile, pour un citoyen, de savoir quelle institution détient des informations

---

[213] A. Toffler, *Les nouveaux pouvoirs. Savoir, richesse et violence à la veille du XXIème siècle*, Paris, Fayard, 1994, p. 344.

[214] Recommandation CM/Rec(2010)13 précitée.

[215] C. de Terwangne, « Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles », *Les petites affiches*, 2005, p. 44 ; J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, *op. cit.*, p. 36 ; CPVP, avis n° 01/2007 relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances, p. 9.

[216] Voy. *infra*, nos 64.- et s.

à son sujet, de quelles informations il s'agit, à qui elles seront communiquées et pour quelle raison.

Outre le fait que cette situation ébranle des impératifs juridiques fondamentaux tels que les exigences de légalité, de transparence et de contrôle de l'administration évoquées précédemment, on craint également des répercussions sur le plan sociologique, étant donné que les technologies modifieraient les comportements individuels.

Sans réaliser une étude fouillée de cette importante question[217], ce phénomène peut se résumer comme suit. N'ayant pas la maîtrise de ses données personnelles, l'individu ignore l'usage qui va être fait de ces informations et craint une utilisation qui lui serait néfaste. Il peut ainsi ressentir une certaine pression psychologique qui le pousse à adopter le comportement le plus conventionnel possible, de manière à ne pas attirer l'attention sur sa personne.

C'est l'argument avancé par la Cour constitutionnelle allemande en 1983 déjà, dans un arrêt important portant sur la constitutionnalité de la collecte, par l'État, de données à caractère personnel nombreuses et précises, dans un but statistique[218]. Elle y affirme que « if someone is uncertain whether information about unusual behavior is being stored

---

[217] Pour la parfaite compréhension des enjeux que cette question fondamentale soulève, les analyses doivent être étendues à l'ensemble des technologies dans tous les domaines de la vie quotidienne, ce qui dépasse largement le cadre de nos réflexions consacrées à l'e-gouvernement. À ce sujet, voy. not., Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in État de droit et virtualité* (Éd. K. BENYEKHLEF et P. TRUDEL), Montréal, Thémis, 2009, pp. 157 à 222 ; A. ROUVROY, « The end(s) of critiques : data-behaviourism vs. Dueprocess », *Privacy, Due Process and the Computational Turn*. (Éd. Mireille Hildebrandt), Ekatarina De Vries, Routledge, 2012 ; A. JONCKEERE, « SIPAR, un système informatique emblématique des transformations observables au sein des maisons de justice », *Champ pénal/Penal field* [En ligne], Séminaire Innovations Pénales, mis en ligne le 31 octobre 2007, disponible sur le site http://champpenal.revues.org/2943 ; DOI : 10.4000/champpenal.2943.

[218] Cour constitutionnelle allemande, 15 décembre 1983, 65 BVerfGE I. Pour une traduction en anglais de cette décision, voy. E. H. RIEDEL, « Federal Constitutional Court Karlsruhe. Census Act 1983 partially unconstitutional », *Human Rights Law Journal,* 1984, pp. 94 à 116. Une traduction en anglais des extraits principaux de cet arrêt figure également dans D.P. KOMMERS, *The constitutional jurisprudence of the Federal Republic of Germany,* 2e éd., Durham and London, Duke University Press, 1997, pp. 324 et 325. Pour un commentaire voy. E.H. RIEDEL, « New bearings in German data protection cenus act 1983 partially unconstitutional », *Human rights Journal,* 1984, pp. 67 à 93 ; T. WÜRTENBERGER et G. SYDOW, « Administration électronique et protection de la vie privée en Allemagne », *in L'administration électornique au service des citoyens. Actes du colloque organisé par le Conseil d'État et l'Université Paris I Panthéon Sorbonne à Paris, les 21 et 22 janvier 2002* (dir. G. CHATILLON et B. DE MARAIS), *op. cit.,* pp. 361 à 372.

and recorded permanently in computer banks, or does not know whether it will be used or passed on, he will try not attract attention engaging in such behavior »[219]. Partant de ce constat, elle interprète le droit à la protection de la vie privée comme le droit de chacun à l' « autodétermination informationnelle », c'est-à-dire, le droit de maîtriser ses propres données en décidant ce qui peut être communiqué, à qui, et ce qu'on peut en faire[220].

Pour illustrer la pression psychologique qui pousse à adopter le comportement le plus normal possible, la Cour constitutionnelle allemande donne l'exemple d'un citoyen qui renoncerait à participer à une réunion ou une manifestation, craignant que cette information soit enregistrée dans un fichier de l'État, et utilisée dans un but qu'il ignore et lui portera peut-être préjudice[221].

Un tel lissage des comportements entraînerait une stigmatisation de la marginalité étant donné que les personnes n'ayant pas le comportement « normal » risqueraient de subir davantage de contrôles, les autorités étant incitées à vérifier que cette « anormalité » n'est pas liée à une fraude quelconque. Ce conformisme imposé porterait atteinte à la liberté de chaque individu de s'épanouir librement, puisqu'il ne se sentirait plus autorisé à se comporter différemment de la majorité de la population. Au-delà, la normalisation des comportements serait également préjudiciable pour la démocratie, qui se nourrit des débats menés entre des personnes ayant des idées divergentes. Il faut admettre, en effet, que « le processus démocratique de décision [...] implique, entre autres, l'expression des préférences des acteurs de la société démocratique ». Il ne peut se réaliser si ces acteurs « n'ont pas la possibilité effective de former et de modifier de manière autonome leur conception du bien, ainsi que de définir en conséquence leurs préférences personnelles »[222].

C'est également ce qu'affirme la Cour constitutionnelle allemande dans l'arrêt précité. Elle soutient que si la protection des données à caractère personnel n'est pas renforcée, le développement technologique « would not only impair his chances of development but would also damage the common good, because self-determination is an elementary fuctional

---

[219] Cour constitutionnelle allemande, 15 décembre 1983, 65 BVerfGE I, tel que repris dans l'ouvrage D.P. Kommers, *The constitutional jurisprudence of the Federal Republic of Germany,* 2e éd., Durham and London, Duke University Press, 1997, p. 325.

[220] Voy. *infra,* nos 64.- et s.

[221] D.P. Kommers, *The constitutional jurisprudence of the Federal Republic of Germany*, *op. cit.*, p. 325.

[222] P. Gerard, *Droit et démocratie. Réflexions sur la légitimité du droit dans la société démocratique*, Bruxelles, Publications des F.U.SL., 1995, pp. 128 à 131.

condition of a free democratic community based on it's citizens ' capacity to act and participate »[223].

51.- Une incitation à la docilité. L'usage des technologies dans l'administration pourrait conduire les citoyens à ne plus contester les règles établies. Comme on l'a vu précédemment, de plus en plus de droits sont octroyés automatiquement aux personnes concernées. Ces dernières ne doivent donc plus faire les démarches pour obtenir l'allocation ou la réduction tarifaire à laquelle elles peuvent prétendre. Bien que cela représente une facilité administrative, le fait que ces individus n'interviennent plus dans le processus administratif signifie aussi qu'ils n'ont plus l'occasion de réfléchir au projet politique qui sous-tend la norme et de le contester, le cas échéant.

Dans le même sens, des outils informatiques guident l'administration dans ses prises de décisions, comme les entrepôts de données permettant les opérations de profilage décrites ci-avant. Leur mode de fonctionnement est le plus souvent incompréhensible pour le citoyen, notamment en raison du fait que ces outils sont fondés sur des calculs algorithmiques complexes. Puisque la population ne comprend pas ces outils, elle s'en désintéresse et, dès lors, ne remet pas en question leur raison d'être.

Comme l'explique Antoinette Rouvroy, « en dépit de son aura d'impartialité et d'objectivité, le tournant numérique semble nous détourner [...] de l'intentionnalité et du 'projet' politique. [...] Alors que dans la présentation qu'en donnait Michel Foucault, le pouvoir, toujours et inévitablement, produit de la récalcitrance, et que la récalcitrance est même un élément absolument essentiel, voire constructif, du pouvoir [perçu comme] un phénomène dynamique, fait d'échanges, de forces et de puissance, la gouvernementalité algorithmique ne *produit* aucune récalcitrance en son sein, dans la mesure où [...] elle évite, préemptivement, toute provocation que la liberté pourrait lui adresser »[224].

Par ailleurs, la docilité des citoyens peut également résulter de contraintes techniques qui empêchent concrètement d'enfreindre la règle. Bien que, pour l'heure, elles ne semblent pas sévir dans l'e-gouvernement belge, ces « technologies de contrôle du comportement humain »[225] sont à craindre, comme l'évoquait récemment la presse[226].

---

[223] Voy. cet extrait de l'arrêt tel que traduit en anglais par D.P. Kommers, *The constitutional jurisprudence of the Federal Republic of Germany, op. cit.*, p. 325.

[224] A. Rouvroy, « Pour une défense de l'éprouvante inopérabilité du droit face à l'opérationnalité sans épreuve du comportementalisme numérique », *Dissensus,* avril 2011, p. 136.

[225] G. Champeau, « Apple et Microsoft veulent rendre l'homme bien sage et docile », 31 août 2012, disponible sur le site www.numerama.com

[226] *Idem.*

> Ainsi, Apple et Microsoft ont obtenu des brevets sur des outils technologiques qui permettent aux autorités publiques, notamment, de désactiver à distance certains appareils.
>
> Plus particulièrement, Microsoft a obtenu en 2008 un brevet pour faire respecter les *Device Manners Policy* (c'est-à-dire, les « bonnes manières »). L'ambition poursuivie est notamment de mettre au point un outil permettant de faire respecter automatiquement les limitations de vitesse, ou d'enclencher les phares dans les tunnels.

Ces technologies qui permettent de contrôler les comportements humains menacent la démocratie et les libertés individuelles. D'une part, elles empêchent la désobéissance, qui est pourtant nécessaire à certains moments. D'autre part, « les régimes autoritaires ou les démocraties en dérive seront effectivement les premières à vouloir s'emparer de ces outils de contrôle pour, ici, empêcher des populations insurgées de communiquer entre elles. Là, pour empêcher un journaliste ou un témoin quelconque de prendre des images qui dérangent »[227].

III. La technocratie

52.- Des questions complexes. L'e-gouvernement fait naître la crainte d'une technocratie, qui se heurte à l'importance du débat démocratique dans un État de droit. Cette matière complexe renforce le « désenchantement du parlementarisme »[228] qui est en marge depuis longtemps et est notamment lié au caractère de plus en plus technique des politiques menées. L'organisation d'outils informatiques suscite nombre de questions complexes, faisant appel à des connaissances techniques parfois poussées ainsi qu'à un vocable particulier, fait d'abréviations étranges et de concepts inédits. Ces difficultés peuvent donner un aspect très obscur aux questions juridiques discutées[229].

> Ainsi, quelles « corrélations » convient-il d'établir entre les données stockées dans un « datawarehouse » en vue du fonctionnement de « Oasis »[230] ? Qui

[227] *Idem.*

[228] X. Bioy et P. Raimbault, « La puissance de la Loi en question », *in La puissance publique à l'heure européenne* (dir. P. Raimbault), Paris, Dalloz, 2006, p. 104.

[229] En ce sens, A. Toffler, *op. cit.*, pp. 342-343.

[230] À ce sujet, voy. L.-A. Traufler et L. Gathy, « Infoshop 4. Organisation anti-fraude des services d'inspection sociale. Datawarehouse O.A.S.I.S. », présentation dans le cadre de la 4e conférence sur la qualité des services publics en Belgique, 20 novembre 2007. Cet exposé est disponible sur le site http://www.epractice.eu/files/documents/cases/1570-1216132007.pdf

doit définir le contenu d'une « source authentique de données »[231] ? Quelle est la différence entre l' « intégrateur de services » et l' « intégrateur de données »[232] ? Comment « synchroniser » les « données d'identification » contenues dans la Banque-Carrefour de la sécurité sociale et au Registre national [233]? Faut-il mettre en place un *audit trail* et donner accès aux *logs*[234] ?

Face à de telles questions, les parlementaires et les ministres chargés de dossiers relatifs à l'e-gouvernement peuvent se sentir découragés. N'ayant peut-être pas le temps ni le courage de s'intéresser à ces sujets arides et à leurs implications cachées, ils préfèrent en appeler à des experts. Ces derniers rédigeront, dans l'ombre, le projet de loi. Le Ministre concerné, faisant aveu de sa méconnaissance du dossier, l'approuvera, tandis que les débats au Parlement pâtiront de leur technicité et pourraient souffrir d'un manque d'intérêt de la part des représentants du peuple. Ces dérives ne sont pas propres à l'e-gouvernement mais elles se révèlent ici avec une acuité particulière.

53.- La crainte d'un manque d'indépendance. S'il faut saluer l'apport d'un expert à propos de ces questions techniques, il y a lieu également de demeurer attentif à ce phénomène nouveau. Les experts ne sont pas nécessairement neutres et peuvent, au travers de leur expertise concernant l'organisation des outils informatiques dans l'administration, faire droit à un intérêt politique particulier voire à un intérêt commercial[235].

54.- La crainte de l'efficacité à tout prix. Outre la question de la neutralité des experts, peut se poser celle de leur méthode de travail. Les experts chargés de rendre l'outil fonctionnel auront à cœur d'être efficaces et rationnels. En d'autres termes, « derrière une scène politique offerte au regard de tous, [...] on découvre la réalité cachée de l'administration technicienne pour qui la poursuite de l'efficacité passe avant toute autre considération. C'est dans la recherche d'une plus grande rationalité technique qu'elle trouve la justification de la clandestinité de son action et le moyen d'imposer ses vues »[236].

---

[231] À ce sujet, voy. not. CPVP, recommandation n° 09/2012 du 23 mai 2012 relative aux sources authentiques de données dans le secteur public.

[232] À ce sujet, voy. not. CPVP, recommandation n° 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public.

[233] À ce sujet, voy. CPVP, avis n° 14/2005 du 28 septembre 2005 faisant suite à une décision d'évocation dans les dossiers SCSZ/05/70, SCSZ/05/90, SCSZ/05/110 et SCSZ/05/113 transmise par le Président du Comité sectoriel de la Sécurité sociale.

[234] À ce sujet, voy. *infra,* nos 400.- et s.

[235] A. Toffler, *op. cit.,* p. 343.

[236] A. Vitalis, *op. cit.,* p. 107.

Ce faisant, l'Homme, et avec lui, ses idéaux, ses convictions politiques, son vécu psychologique, risquent d'être considérés comme le principal obstacle de cette révolution technologique et des choix mathématiques qui l'accompagnent. « Il faut organiser une 'société de l'information totale', une nouvelle 'civilisation de la logique', [...] dans lesquelles ne sera tolérée aucune survivance religieuse, aucune croyance, aucune domestication idéologique [...]. [Il faut] rendre le progrès inéluctable en…l'automatisant. [...] L'homme n'est plus un obstacle au changement, il en devient un simple spectateur. C'est le rêve d'une révolution logique et propre, réalisée par la machine, loin des tumultes de la politique et de l'idéologie, pour une humanité passive et inerte »[237]. « Ce n'est pas la domination par l'homme de ses conditions d'existence, c'est au contraire l'adaptation de celui-ci à une évolution qui lui est étrangère »[238].

IV. Les failles dans la sécurité informatique

55.- Des problèmes techniques. Malgré les apparences, un outil informatique n'est pas infaillible. Le fonctionnement de l'e-gouvernement est donc susceptible d'être affecté par des problèmes techniques qui mettent en péril la sécurité informatique. On pense notamment aux atteintes portées à la fiabilité des données, à la confidentialité de celles-ci, ainsi qu'à la disponibilité du système informatique[239].

56.- Les risques pour la fiabilité des données. Depuis toujours, les administrations collectent, encodent et utilisent des informations relatives aux citoyens pour accomplir leurs missions. L'utilisation de l'informatique dans les administrations permet aujourd'hui de diminuer certaines erreurs commises jadis.

---

[237] A. Vitalis, *op. cit.,* p. 23. Voy. aussi M. P. Juvigny, « Les réalisations scientifiques et techniques modernes et leurs conséquences sur la protection du droit au respect de la vie privée et familiale, du domicile et des communications », *in Vie privée et droits de l'homme. Actes du 3e colloque international sur la Convention européenne des droits de l'homme (Bruxelles 30 septembre – 30 octobre 1970),* Bruxelles, Bruylant, 1973, p. 180.

[238] P. Alembick, *Informatique et idéologie*, cité par A. Vitalis, *op. cit.*, p. 23.

[239] La fiabilité et la confidentialité des données ainsi que la disponibilité des systèmes informatiques sont trois éléments qui composent l'impératif de « sécurité informatique », qui peut être défini comme « l'obtention et la conservation de la confidentialité, de l'intégrité, de la disponibilité, de l'imputabilité, de l'authenticité, de la fiabilité et de la non répudiation de l'information et des équipements de traitement de l'information » [Norme ISO/IEC 13335-1 :2004 – Information technology — Guidelines for the management of IT Security —Part 1 : Concepts and models for information and communications technology security management].

> Par exemple, grâce aux sources authentiques de données, les informations sont enregistrées dans une seule base de données. Puisqu'une administration est responsable de la fiabilité des données qui s'y trouvent, leur mise à jour est en principe garantie et on diminue le risque de prendre des décisions à partir d'informations dépassées.
>
> Un autre exemple est l'encodage informatisé des informations qui diminue le risque de fautes dans l'orthographe du nom ou de l'adresse du citoyen.

Toutefois, tous les dangers n'ont pas disparu car des erreurs peuvent encore survenir lors de l'encodage des informations. Ces erreurs ont alors un impact d'autant plus grand que l'e-gouvernement est fondé sur l'utilisation des sources authentiques et le principe de la collecte unique des données : puisque la donnée a vocation à être réutilisée au maximum, l'erreur qui l'affecte sera démultipliée d'autant. En outre, un temps long peut s'écouler avant que l'erreur ne soit dénoncée et corrigée, puisque ces réutilisations se produisent sans passer par le contrôle du citoyen concerné. Ce dernier n'a connaissance de l'erreur produite qu'à partir du moment où il est mis en contact avec la donnée erronée, ce qui n'arrive souvent qu'une fois adoptée la décision administrative fondée sur ladite information.

> Par exemple, depuis 2006 se met en place l'échange informatique de données entre le SPF Finances et le SPF Sécurité sociale. Pour calculer les aides et les allocations auxquelles certaines catégories de citoyens ont droit, le SPF Sécurité sociale doit demander des informations au SPF Finances, pour connaître, notamment, l'importance des ressources du demandeur, qu'il s'agisse du revenu ou de la propriété de biens immobiliers. Si les données détenues par le SPF Finances sont erronées, l'erreur affectera non seulement les décisions prises par le SPF Finances, mais également celles du SPF Sécurité sociale, entraînant des décisions peut-être inopportunes et beaucoup de tracasseries administratives pour la personne concernée.
>
> En France, la CNIL a récemment dénoncé les erreurs affectant de multiples données enregistrées dans le STIC[240], pointant notamment le manque de mise à jour systématique de celles-ci, dû, entre autres, à l'absence récurrente de transmission, par les parquets, des suites judiciaires nécessaires à la mise à jour du STIC, telles que les classements sans suite, acquittement, non-lieu etc. Ainsi, seules 17 % des fiches des personnes y répertoriées seraient exactes. Or, cette base de données peut avoir des conséquences sociales considérables puisqu'elle est notamment utilisée à l'occasion du recrutement ou de l'habi-

[240] Il s'agit du « système de traitement des infractions constatées », un fichier national placé sous la responsabilité du Ministre de l'Intérieur. Cet outil remplit une double fonction : d'une part, identifier les auteurs d'infractions et établir des statistiques d'analyse de l'activité de police ; d'autre part, servir d'instrument d'enquête administrative.

litation d'environ un million d'emplois. Etre fiché dans le STIC peut donc entraîner la perte d'emploi, le refus d'embauche, l'impossibilité de passer un concours administratif, etc.[241].

57.- Les risques pour la confidentialité des données. Le risque existe que des personnes prennent connaissance des données personnelles des citoyens alors qu'elles n'en ont pas le droit. Cela peut arriver en cas de piratage informatique. Tout système informatique, même perfectionné, risque d'être un jour « craqué ».

Par exemple, à la fin du mois de janvier 2011, le site internet du Gouvernement wallon a été piraté par un groupement qui s'intitule « MOH Mouvement Offensive Hacker Underground »[242]. Ce fait a très rapidement suscité un certain émoi, vu la crainte que les pirates aient pu accéder à la partie du site internet contenant les documents confidentiels. Heureusement, en l'espèce, aucune information confidentielle n'a été volée mais ce fait montre la faillibilité du site internet d'une importante autorité publique.

D'ailleurs, avant ce cas, d'autres piratages informatiques importants ont visé le site internet d'administrations de grande envergure. Ils se sont d'ailleurs avérés particulièrement problématiques notamment parce que les pirates utilisaient un virus de type « cheval de Troie » leur permettant notamment d'enregistrer des mots de passe pour pénétrer davantage le système informatique. Ainsi, par exemple, la Commission européenne[243], le Ministère français des Finances[244] et le Ministère des Finances canadien[245] ont été victimes d'une sérieuse *cyber*attaque.

---

[241] CNIL, Conclusions du contrôle du système de traitement des infractions constatées (STIC), Rapport remis au Premier ministre le 20 janvier 2009, http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Controles_Sanctions/Conclusions%20des%20controles%20STIC%20CNIL%202009.pdf

[242] À ce sujet voy. Information Belga, « Le piratage du site internet du gouvernement wallon destiné au public », *La Libre,* 31 janvier 2011, disponible sur le site http://www.lalibre.be/societe/cyber/article/639608/piratage-du-site-internet-du-gouvernement-wallon-destine-au-public.html

[243] AFP, « La Commission européenne victime d'une cyberattaque », *Le Soir,* 23 mars 2011, disponible sur le site http://www.lesoir.be/actualite/vie_du_net/2011-03-23/la-commission-europeenne-victime-d-une-cyber-attaque-830149.php

[244] Belga, « France : le ministère de l'économie victime d'une cyberattaque », *La Libre,* 7 mars 2011, disponible sur le site http://www.lalibre.be/actu/international/article/647284/france-le-ministere-de-l-economie-victime-d-une-cyberattaque.html

[245] À ce sujet, voy. not. « Intrusion informatique : avant Bercy, le ministère du trésor canadien », *Le Monde,* 7 mars 2011, http://www.lemonde.fr/technologies/article/2011/03/07/intrusion-informatique-avant-bercy-le-ministere-du-tresor-canadien_1489422_651865.html

Par ailleurs, des agents de l'administration peuvent céder à la curiosité en consultant des données personnelles de citoyens alors que l'exercice de leurs missions ne le requiert pas.

> On pense, par exemple, à la consultation du registre DIV par des policiers ayant repéré, sur la route, de jolies conductrices à qui ils désirent téléphoner, ou encore à la consultation du Registre national par un fonctionnaire communal dans le but de retrouver l'adresse de son ancienne compagne[246].

Enfin, il peut être tentant d'utiliser des informations dans un autre but que celui pour lequel elles ont été collectées initialement. Il s'agit alors d'un détournement de finalité[247].

> Par exemple, il y a quelques années, la Bourgmestre de Huy s'est vu reprocher le fait d'utiliser les coordonnées des patients tout juste sortis du CHR de Huy pour leur envoyer une carte de prompt rétablissement, ainsi que les données des personnes d'origine étrangères, pour les convier à des réunions d'information sur le vote des étrangers[248].

58.- Les risques pour la disponibilité du système informatique. Un système informatique n'est jamais à l'abri de pannes informatiques. Celles-ci sont préjudiciables tant pour l'administration, qui est soumise à l'exigence de la continuité du service public, que pour les citoyens, tenus d'accomplir leurs démarches administratives dans les délais impartis.

> Par exemple, à plusieurs reprises, le système *Tax on web*, qui permet de remplir sa déclaration fiscale en ligne, a subi des pannées dans les jours qui précédaient l'échéance de la remise de la déclaration d'impôts[249].

*

Conclusions

Après avoir circonscrit la notion d'e-gouvernement, trois outils particulièrement importants dans ce contexte nouveau ont été définis et illustrés, à savoir la source authentique, la plateforme d'échanges d'informations et le numéro d'identification.

---

[246] À ce sujet, voy. not., C.E., *Van Merris,* arrêt n° 143.683 du 26 avril 2005.

[247] Voy. *infra,* n° 124.-

[248] Voy. C.E., *Lizin,* n° 211.698 du 2 mars 2011. Voy. *infra,* n° 479.-

[249] Voy. not., la question n° 347 de M. Kattrin Jadin du 28 avril 2011 (F), *Q.R.,* Chambre, session 2010-2011, 6 juin 2011, pp. 6 et 7.

Ces outils permettent aux administrations de s'échanger aisément, et de manière fiable, les données à caractère personnel des citoyens. Ils répondent ainsi au principe de la collecte unique des données qui sous-tend le développement de l'e-gouvernement. Des opérations nouvelles au sein de l'administration sont également rendues possibles, comme en témoignent les exemples du profilage et de l'automatisation des droits. De toute évidence, ces techniques et ces opérations renforcent l'efficacité administrative, tant au bénéfice des administrations que des citoyens.

Si ce constat génère, certes, beaucoup d'enthousiasme, il fait naître aussi des craintes nouvelles car l'e-gouvernement bouleverse le fonctionnement traditionnel de l'administration. En particulier, on voit surgir aujourd'hui le risque d'un renforcement du pouvoir de l'État et d'un déséquilibre important entre l'administration et le citoyen. Ce déséquilibre risque de générer une normalisation des comportements des individus. Dans ce contexte, la démocratie est menacée. Elle l'est même d'autant plus que s'instaure progressivement une technocratie, aux mains des experts. Il ne faut pas oublier non plus que, malgré les apparences, les outils technologiques ne sont pas infaillibles, si bien que les atteintes à la sécurité informatique ne peuvent être exclues.

De telles craintes doivent être entendues par le législateur et rencontrées par les règles de droit. À cet égard, le régime juridique de la protection de la vie privée et des données à caractère personnel mérite une attention particulière. Il fait l'objet du deuxième chapitre.

*

CHAPITRE II.
La protection de la vie privée et des données à caractère personnel

Introduction

59.- La protection de la vie privée et des données à caractère personnel applicable à l'e-gouvernement. À la lecture du premier chapitre, on perçoit d'emblée qu'une base de données n'est pas la simple modernisation d'un fichier papier, qu'un échange électronique de données n'équivaut pas à l'envoi de la photocopie d'un document par la poste, que la détection des fraudes rendue très efficace grâce aux technologies ne s'assimile pas à un raisonnement humain.

Ce constat provoque un certain malaise. On sent que l'e-gouvernement menace l'intimité des citoyens, en offrant à l'État les moyens d'en savoir toujours plus sur chaque personne. L'e-gouvernement met également en péril la capacité des individus à comprendre l'environnement administratif qui les entoure. Comment savoir quelle donnée se trouve à quel endroit et ce qu'on va en faire ?

C'est pour répondre aux craintes générées par les développements technologiques qu'ont été dessinées les règles de protection des données, ancrées dans une valeur fondamentale pour l'homme, la vie privée. C'est pourquoi, un traitement de données à caractère personnel – tel que l'enregistrement de données par l'administration – est considéré comme une ingérence dans la protection de la vie privée des citoyens[250].

[250] Remarquons également qu'un outil informatique « constitue une intrusion corrélativement plus importante dans les droits [...] au respect de la vie privée et à la protection des données à caractère personnel » que les outils traditionnels [Conclusions de l'avocat général E. Sharpston, du 17 juin 2010, § 96, sous C.J.U.E., gde ch., 9 novembre 2010, *Volker und Markus Schecke* et *Eifert GbR et Hartmut Eifert*, aff. jointes C-92/09 et C-93/09. Pour un commentaire de cet arrêt, voy. E. Degrave, « Arrêt 'Volker und Markus Scheke GbR et Harmut Eifert' : le droit fondamental à la protection des données à caractère personnel et la transparence administrative », *J.D.E.,* 2011, pp. 97-99]. Dans le même sens, voy. les travaux préparatoires de la loi du 8 décembre 1992 : projet de loi relatif à la protection de certains aspects de la vie privée, *Doc. Parl.* Ch. Repr., sess. 1983-1984, n° 778, p. 14.

> Dans son arrêt *Amann c. Suisse*, notamment, la Cour européenne des droits de l'homme se prononce sur la conformité, au regard de l'article 8 de la Convention européenne des droits de l'homme, de l'établissement d'une fiche reprenant le contenu d'une conversation téléphonique. Elle affirme que « la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieure des informations mémorisées importe peu »[251].

Dès lors, pour être effectué en toute légalité, un tel traitement d'informations doit respecter les conditions fixées par le régime juridique de la protection des données à caractère personnel.

> À cet égard, l'arrêt *Rotaru contre Roumanie,* rendu le 4 mai 2000 par la Cour européenne des droits de l'homme, mérite une attention particulière. Cette affaire concerne la détention, par les services de renseignements roumains, de données personnelles relatives à l'activité politique du requérant. La Cour européenne des droits de l'homme y affirme notamment que « des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique recueillies et mémorisées dans les fichiers tenus par les pouvoirs publics » et elle définit les règles que la protection de la vie privée impose à ce type de traitement de données[252].

Après avoir expliqué l'ancrage de la protection des données à caractère personnel dans le droit fondamental à la vie privée, des développements sont consacrés aux notions cardinales de ce régime juridique.

*

Section 1. Le lien entre la protection des données à caractère personnel et la protection de la vie privée

60.- Considérations générales. La protection des données à caractère personnel a été conçue comme un outil au service d'une valeur, la vie privée des citoyens. Elle constitue aujourd'hui un régime juridique spécifique composé de plusieurs normes distinctes.

---

[251] Cour eur. D.H., *Amann c. Suisse,* 16 février 2000, req. n° 27798/95, § 65.

[252] Cour eur. D.H., *Rotaru c. Roumanie,* 4 mai 2000, req. n° 28341/95, § 43. Nous y reviendrons dans le premier titre de la recherche consacré à la légalité des traitements de données. Voy. *infra,* n° 103.-

I. La protection des données à caractère personnel : un outil au service d'une valeur, la vie privée

61.- La raison d'être des règles de protection des données. La protection des données à caractère personnel désigne l'ensemble des règles qui encadrent l'utilisation des données à caractère personnel des individus[253].

Ce régime juridique a été créé pour garantir la protection des personnes face aux développements informatiques. Il est donc un outil au service d'une valeur[254]. C'est la raison pour laquelle ces règles s'ancrent dans le droit fondamental à la protection de la vie privée, consacré par l'article 8 de la Convention européenne des droits de l'homme et, en Belgique, par l'article 22 de la Constitution.

Le lien entre la protection des données à caractère personnel et la protection de la vie privée ne s'impose pas nécessairement avec la force de l'évidence. C'est particulièrement le cas dans le secteur public où, souvent, les individus peinent à comprendre le lien existant entre l'utilisation des données *a priori* « banales » détenues par les administrations – telles que leur adresse ou leur date de naissance – et la menace que le traitement d'une telle information représente pour leur vie privée. Feignant l'indifférence, ils arguent du fait qu'ils n'ont « rien à cacher »[255].

Pour comprendre un tel lien, il faut savoir que les règles organisant les traitements de données à caractère personnel visent à protéger le développement personnel de tout individu, menacé par les technologies. Ces règles s'enracinent dans la protection de la vie privée, compte tenu de la richesse de ce droit fondamental tel qu'on l'interprète aujourd'hui.

A. Des règles pour protéger le libre développement personnel face aux technologies

62.- Des craintes kafkaïennes. Comme on l'a dit précédemment, depuis l'apparition de l'informatique et des traitements de données à caractère personnel, de plus en plus de données à caractère personnel sont collectées et soumises à des traitements de plus en plus nombreux, au sein de l'administration notamment. Le fait que les données personnelles

[253] La notion de donnée à caractère personnel est définie au n° 70.-

[254] Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in État de droit et virtualité* (dir. K. Benyekhlef et P. Trudel), Montréal, Thémis, 2009, p. 169.

[255] Sur ce constat, voy. D. Solove, « I've got nothing to hide' and other misunderstandings of privacy », *op. cit.,* pp. 746 et 747.

des citoyens soient utilisées par l'État requiert une attention minutieuse, pour deux raisons en particulier. D'une part, les données collectées par les administrations sont multiples et touchent à de nombreux aspects de la vie de chaque citoyen. L'État détient donc suffisamment d'informations pour avoir une vue très précise de chaque citoyen. D'autre part, dans leurs relations avec les administrations, les individus ne peuvent choisir de communiquer, ou non, leurs informations personnelles. Ils y sont contraints, sous peine de ne pas bénéficier de la prestation de service public demandée[256] voire même, de ne pas exister aux yeux de l'administration[257]. Il est donc particulièrement important que l'usage des données par les administrations soit encadré et que les citoyens n'aient pas à craindre que l'État commette des abus dans l'utilisation de leurs données.

Or, on a pointé ci-avant que l'informatisation de l'administration crée un déséquilibre important entre l'administration et le citoyen. Par conséquent, l'individu est susceptible d'être soumis à des décisions prises sur la base d'informations dont il n'a plus la maîtrise. Il ne peut pas vérifier leur exactitude ni la raison pour laquelle on les a collectées. Il n'a pas non plus connaissance des autorités à qui elles sont communiquées, pour quelles raisons, à quel moment, ni pendant combien de temps elles sont conservées. Dans ce contexte, le citoyen risque de vivre un sentiment d'absurdité, ne comprenant plus et ne contrôlant plus le fonctionnement de l'administration qui prend des décisions le concernant. Cette situation fait penser à celle dépeinte dans *Le Procès,* de Kafka.

Cette comparaison est faite par Daniel Solove, qui estime que la métaphore du *Big Brother* de Georges Orwell permet, certes, d'expliquer les dangers des outils technologiques visant à surveiller les citoyens, mais elle ne rend pas assez compte des risques liés à l'utilisation de données *a priori* banales, telles que la date de naissance, l'adresse, etc. A juste titre selon nous, Daniel Solove estime que la métaphore du Procès de Kafka est mieux adaptée aux craintes générées par les traitements de données à caractère personnel dans le secteur public car elle permet d'illustrer le déséquilibre créé entre des administrations puissantes et des citoyens vulnérables[258]. En effet, dans cet ouvrage, Kafka décrit « a bureaucracy with inscrutable purposes that uses people's information to make important

[256] Par exemple, une personne handicapée est obligée de fournir un certain nombre de détails sur son handicap pour bénéficier de l'allocation qu'elle réclame.

[257] Sans même prétendre à l'obtention d'une allocation, tout citoyen est contraint d'être enregistré dès sa naissance dans le Registre national, qui contient 13 informations d'identification à son sujet.

[258] D. SOLOVE, « I've got nothing to hide' and other misunderstandings of privacy », *op. cit.,* p. 757.

decisions about them, yet denies the people ability to participate in how their information is used »[259]. Si on ne protège pas suffisamment les données des citoyens, l'e-gouvernement risque de s'apparenter à pareille bureaucratie.

Une telle situation menace le libre épanouissement de chaque citoyen et conduit à la normalisation des comportements, que l'on a précédemment pointée comme étant l'une des craintes majeures dans l'e-gouvernement.

63.- Garantir le contrôle du citoyen sur l'administration. Un État démocratique ne peut tolérer les risques engendrés par le développement d'une administration kafkaïenne et, plus particulièrement, le déséquilibre important qui affecte la relation entre l'administration et le citoyen. Face à ces craintes, les règles de protection des données constituent un outil permettant au citoyen d'exercer un contrôle sur la personne, publique ou privée, qui traite ses données à caractère personnel.

C'est pourquoi, les règles de protection des données octroient des droits aux individus concernés par les traitements de données, pour connaître et contrôler l'utilisation qui est faite de leurs informations étant donné qu'« une condition indispensable à la libre construction, par l'individu, de sa propre personnalité, est qu'il puisse être certain que les informations [...] personnelles qui le concernent ne soient obtenues et utilisées d'une manière qui échappe totalement à son contrôle »[260]. Par exemple, la personne concernée a le droit d'exiger la communication des données à caractère personnel que le responsable du traitement détient à son sujet.

> Lors des discussions préparatoires à l'adoption de la loi du 8 décembre 1992, il a été affirmé que l'informatisation n'est pas « le croque-mitaine de la vie privée »[261]. Dès lors, les règles de traitements de données veillent « à assurer un équilibre entre les nécessités de la protection de la vie privée et celles d'une politique administrative, économique et sociale bien organisée. Les obligations imposées au [responsable du traitement] sont établies de façon à ce que les charges soient réduites sans porter atteinte aux droits des particuliers »[262].

---

[259] *Ibid.*, p. 756.

[260] Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *op. cit.*, p. 209.

[261] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel et proposition de loi relative à la protection de données personnelles concernant les personnes physiques dans les fichiers informatiques ou banques de données et à la création d'une commission nationale de l'informatique et des libertés, Rapport fait au nom de la Commission de la Justice par Mme Merckx-van Goey, *Doc. Parl.*, Chambre, session 1991-1992, n° 413/12, p. 3.

[262] *Ibid.*, p. 6.

Les règles de protection des données imposent également des limites à la personne ou l'autorité qui traite des données à caractère personnel et que l'on appelle le « responsable du traitement »[263]. Par exemple, le responsable du traitement doit respecter l'exigence de finalité, en vertu de laquelle les données ne peuvent être récoltées que pour satisfaire un objectif précis et légitime. Ces limites et ces droits sont au cœur d'amples développements dans la suite de la présente recherche, raison pour laquelle nous ne les approfondissons pas dans ce chapitre introductif.

Par ailleurs, le souci de baliser l'utilisation des données des citoyens conduit à structurer l'e-gouvernement de manière décentralisée. En mettant en place des réseaux sectoriels, des sources authentiques de données et des plateformes d'échanges d'informations, on maintient les barrières nécessaires pour éviter les abus dans le traitement des données, tout en confortant l'efficacité administrative puisqu'on facilite la circulation électronique des données[264]. Comme on l'a dit précédemment[265], une telle décentralisation des informations évite la création d'une gigantesque base de données aux mains de l'État, qui rendrait les pouvoirs publics très puissants puisqu'ils auraient accès, en quelques « clics », à l'ensemble des informations sur l'ensemble des individus. Il serait alors beaucoup plus difficile de contrôler la légalité des accès aux données et d'éviter les abus dans l'utilisation de ces informations personnelles.

En France, un tel projet de centralisation des données des citoyens a été envisagé en 1973. Ce projet s'appelait SAFARI, acronyme de « système automatisé pour les fichiers administratifs et le répertoire des individus ». Il a rapidement été qualifié d'outil de « chasse aux français »[266]. Il consistait à utiliser un numéro d'identification unique pour l'ensemble des fichiers publics, de manière à faciliter le regroupement des informations de chaque individu[267]. Le projet SAFARI a suscité beaucoup d'émoi. Il a donné lieu à la mise en place d'une commission parlementaire, qui a débouché sur un rapport assez alarmiste de Bernard Tricot et Pierre Catala. Les auteurs y affirment notamment qu' « on entend dire souvent qu'il est temps de désenclaver les différents services de l'administration par la diffusion et l'échange des informations. C'est une formule qui ne nous paraît pas indiscutable. S'il est vrai qu'il faut abattre des barrières, il en

[263] Sur cette notion, voy. *infra,* n°s 73.- et 75.-

[264] Nous reviendrons sur ce point ulétérieurement au sujet de la notion de *Privacy by design*. Voy. *infra,* n°s 158.- et s.

[265] Voy. *supra*, n°s 15.- et s.

[266] Comme l'a titré à l'époque le journal *Le Monde*.

[267] H. Maisl, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », *op. cit.,* p. 350.

est aussi d'utiles et de nécessaires. Le jour où, au sein de l'État, chaque fonctionnaire qui détient une parcelle de la puissance publique pourrait tout savoir de chaque homme, de chaque famille, de chaque entreprise, ne voit-on pas à quels risques l'administré serait exposé ? »[268].

Le projet SAFARI a ensuite été abandonné. Suite au rapport de la commission parlementaire, a été adoptée la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui impose les conditions de traitements de données à caractère personnel et institue l'autorité de protection des données française, la Commission nationale Informatique et Libertés (dite « CNIL »).

B. Des règles enracinées dans le droit fondamental à la protection de la vie privée

64.- La protection des données enracinée dans la protection de la vie privée. D'emblée, les questions de protection des données ont été rattachées au droit fondamental à la protection de la vie privée.

> Par exemple, la Convention n° 108, adoptée le 28 janvier 1981, organise la protection des données à caractère personnel[269]. Le préambule de cette Convention justifie l'adoption de règles applicables aux traitements de données par le souhait « d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée ». Le droit au respect de la vie privée y reçoit une attention particulière, étant affirmé explicitement alors que les autres droits ne le sont pas. Le souci de ne pas porter atteinte à la vie privée des citoyens est également évoqué dans de nombreuses discussions ayant précédé l'adoption des premières lois belges relatives à la protection des données[270]. Par ailleurs, dans l'arrêt *Rotaru c. Roumanie,* la Cour européenne des droits de l'homme consacre le lien entre la protection de la vie privée et la protection des données à caractère personnel[271].

Pourquoi enraciner la protection des données dans un droit fondamental, et dans le droit fondamental à la protection de la vie privée, en particulier ? Que penser alors du droit autonome à la protection des données, consacré récemment par la Charte des droits fondamentaux de

[268] Rapport de la Commission Informatique et Libertés, 1975, T. I., p. 17.

[269] Voy. *infra,* n° 66.-

[270] Voy. not. les discussions parlementaires qui ont précédé l'adoption de la loi du 15 janvier 1991 sur la Banque-Carrefour de la sécurité sociale et l'adoption de la loi du 8 décembre 1992.

[271] Cour eur. D.H., *Rotaru c. Roumanie,* 4 mai 2000, §43.

l'Union européenne ? Telles sont les questions que renferment les lignes qui suivent.

a) Pourquoi enraciner la protection des données dans un droit fondamental ? La première raison est *procédurale*. On ne pourrait soumettre une question de protection des données à la Cour européenne des droits de l'homme, ou à la Cour constitutionnelle, sans invoquer la violation d'un droit fondamental à l'appui de l'argumentation. Or, ni la Convention européenne des droits de l'homme, ni la Constitution, ne consacrent un droit autonome à la protection des données. Il faut donc passer par le droit fondamental à la protection de la vie privée.

La deuxième raison est *idéologique*. La protection des données n'est pas une valeur en elle-même. L'équilibre que tentent d'instaurer les règles de protection des données, entre le responsable du traitement et la personne dont les données sont traitées, n'existe pas dans l'absolu. Il faut donc définir cet équilibre par rapport à un idéal à atteindre et en fonction d'un contexte particulier. Pour concrétiser cette idée, remarquons qu'une même question de protection des données peut être résolue différemment selon le responsable du traitement en cause et les enjeux sous-jacents à la question soulevée.

> Par exemple, un responsable de traitement a collecté la date de naissance et l'adresse d'une catégorie d'individus. Peut-on réutiliser cette information ?
>
> Si le responsable du traitement est le chef d'un petit orchestre d'amateurs, qui a demandé la date de naissance et l'adresse de ses musiciens lors de la première répétition, et souhaite ensuite réutiliser ces informations pour leur envoyer une carte d'anniversaire le jour J, on est tenté de dire que la réutilisation de ces données ne porte pas atteinte à la vie privée du musicien concerné et ne déséquilibre pas la relation entre le responsable du traitement et le musicien.
>
> Par contre, si le responsable du traitement est une commune, qui connaît l'adresse et la date de naissance des citoyens car ceux-ci ont dû obligatoirement la communiquer pour être enregistrés au Registre national, et qu'elle souhaite réutiliser la date de naissance et l'adresse pour faire la publicité des écoles communales auprès des parents des enfants de 5 ans, ou vendre à une société de chirurgie esthétique le nom de toutes les habitantes de la commune de plus de 30 ans susceptibles d'être intéressées par des implants mammaires, on est nettement plus mal à l'aise. Le fait, notamment, qu'il s'agisse d'une autorité publique et que les données ont dû obligatoirement être communiquées par les individus, rend l'examen du traitement plus délicat que dans l'exemple précédent, bien qu'il s'agisse des mêmes données. Si de tels traitements devaient être réalisés par la commune, on devrait y voir une atteinte à la protection de la vie privée. Il y aurait un déséquilibre entre la commune, qui abuse des données dont

elle dispose, et les personnes concernées qui subiront les conséquences de ces traitements.

b) Pourquoi enraciner la protection des données dans la protection de la vie privée, plutôt que dans un autre droit fondamental ? Protéger l'utilisation des données personnelles des citoyens permet de protéger leur vie privée, mais également d'autres droits fondamentaux.

> Par exemple, en encadrant l'utilisation des données relatives à l'origine ethnique et à la santé, on protège le droit à l'égalité et à la non-discrimination. En limitant l'utilisation des données relatives à l'appartenance syndicale, on protège la liberté d'association. Régler l'usage des données relatives à l'appartenance religieuse encourage la liberté de culte, etc.[272].

Néanmoins, la vie privée est une valeur particulièrement propice pour guider la protection des données. Pour le comprendre, il importe de saisir pleinement les deux versants de la vie privée.

Il y a, d'une part, la vie privée « solitaire ». C'est le droit d'être laissé seul. À cet égard, l'État a une obligation négative, celle de ne pas intervenir dans la sphère intime des citoyens qui peuvent se prévaloir de leur droit à la vie privée entendu de manière « défensive »[273].

> Par exemple, la vie privée, entendue de manière « défensive », est invoquée notamment dans les réflexions relatives aux technologies permettant de surveiller les individus, en s'ingérant dans leur intimité physique, telles que les caméras de vidéosurveillance, les RFID, les GPS, etc.

Il y a, d'autre part, la vie privée « participative ». C'est le droit, pour tout individu, de participer à la vie démocratique en pleine connaissance de cause et de choisir librement « la manière dont il décide de sa vie avec autrui »[274]. C'est l'idée que « le droit à la vie privée [...] n'est pas seulement le droit de rester chez soi pour exclure les autres, c'est aussi le droit de

---

[272] Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *op. cit.,* p. 210.

[273] S.D. Warren et L.D. Brandeis, « The Right to Privacy », *Harvard Law Review,* 1890, p. 193 ; D. Solove, « Coneptualizinf Privacy », *California law review,* 2002, pp. 1095 à 1999 ; D. Solove, « I've got nothing to hide' and other misunderstandings of privacy », *op. cit.,* p. 755.

[274] Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *op. cit.,* p. 204.

sortir de chez soi pour aller vers les autres »[275]. Cela implique l'obligation, pour l'État, de créer les conditions matérielles et psychologiques qui permettent à chacun une telle implication dans la société. Le droit à la vie privée est alors entendu de manière « offensive » puisque chacun peut exiger de l'État qu'il mette en place ces conditions.

> Par exemple, l'État est obligé d'organiser l'accès aux documents administratifs pour permettre à chacun de prendre connaissance des documents administratifs qui les éclairent sur les décisions prises dans leur commune notamment[276].

Ces deux facettes de la vie privée doivent irriguer la protection des données et lui permettre d'atteindre sa raison d'être. Rappelons, en effet, que les règles de protection des données sont créées pour permettre à chacun de s'épanouir librement. Or, ce plein épanouissement personnel suppose que chaque individu ait tant la possibilité de s'isoler, que celle d'interagir avec autrui. C'est « dans cette 'vibration' constante entre besoin de solitude et besoin d'interaction avec autrui que se développe la personnalité individuelle »[277]. Ainsi portée vers l'idéal de la vie privée, la protection des données incarne les conditions nécessaires au développement libre de chaque personne, inspirées de solitude et de participation. Charles Fried ne disait pas autre chose lorsqu'en 1968 déjà, il affirmait que « to respect, love, trust, feel affection for others and to regard ourselves as the objects of love, trust and affection is at the heart of our motion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion »[278].

Dans le même temps, aujourd'hui, la notion de vie privée n'est plus seulement interprétée comme le droit d'être laissé seul, ou le droit d'exiger de l'État qu'il mette en place les conditions matérielles et psychologiques de participation à la vie démocratique. Ce droit fondamental est également entendu comme le droit à l' « autodétermination informationnelle », c'est-à-dire, le droit de tout individu de maîtriser son image

---

[275] J.-P. Marguénaud, *La Cour européenne des droits de l'homme,* 4e éd., Paris, Dalloz, 2008, p. 74.

[276] Au sujet du lien entre protection de la vie privée et obligation d'information, voy. C. de Terwangne, *Société de l'information et mission publique d'information,* thèse de doctorat, Namur, 2000, et en particulier, Partie I, chapitre 2 qui traite notamment de l'arrêt de la Cour européenne des droits de l'homme qui illustre cette problématique (Cour eur. D.H., *Guerra c. Italie,* 19 février 1998).

[277] Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *op. cit.,* p. 210.

[278] C. Fried, "Privacy", *Yale Law Journal,* 1968, vol. 77, pp. 477 et 478.

informationnelle, en décidant lui-même des conditions d'utilisation de celles-ci ou, au moins[279], en ayant connaissance de l'usage qui en est fait[280]. Précisons que, comme l'affirme Cécile de Terwangne, « 'maîtriser' ne signifie pas nécessairement choisir et déterminer ce qui est communiqué à autrui. Il s'agit surtout d'avoir accès aux données conservées et/ou utilisées par d'autres et d'avoir connaissance du sort réservé à ces données »[281].

En définitive, l'autodétermination informationnelle, c'est l'idée que toute personne peut légitimement refuser de dévoiler les informations qui la concernent sans pour autant chercher à cacher des choses répréhensibles, tout comme elle a le droit de placer des rideaux à ses fenêtres sans pour autant que ce fait puisse révéler quelque attitude suspecte. Plus largement, le respect de la dignité et l'autonomie de chacun suppose qu'on ait conscience du fait que nos données sont utilisées, et qu'on puisse connaître et contrôler de telles utilisations.

Si l'autodétermination n'est pas garantie, on risque de ressentir, face à l'administration qui traite toutes nos informations, ce sentiment que l'on éprouve lorsqu'un inconnu s'est immiscé par effraction dans notre maison, même sans rien y voler : un malaise lié au fait que des gens aient pu voir des informations personnelles sans qu'on l'ait choisi ni même su, et qui ne les regardent pas. À la longue, cela peut créer chez les citoyens une peur de s'épanouir librement, d'inventer, d'essayer, de plaisanter, de critiquer, … et générer, au final, des comportements standardisés qui posent question au regard de la liberté de chacun d'être ce qu'il veut être.

---

[279] Cette nuance est liée au fait que, dans l'e-gouvernement notamment, il y a des situations dans lesquelles le citoyen est obligé de donner ses informations personnelles. C'est le cas, par exemple, des données du Registre national qui sont obligatoirement enregistrées à défaut de quoi, le citoyen n'aurait pas d'existence civile.

[280] Dans le même sens, voy. Y. Poullet, « L'informatique menace-t-elle nos libertés ? », *in La télématique, T. 1 : Aspects juridiques, techniques et socio-politiques. Actes du colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit (CRID) des Facultés Notre-Dame de Namur*, Gand, Story-Scientia, 1984, pp. 195 et 196 ; H Burkert, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *Droit de l'informatique et des Télécoms*, 1985, pp. 8 à 16 ; Th. Leonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », *in La vie privée : une liberté parmi les autres ?* (dir. F. Rigaux), Bruxelles, Larcier, 1992, pp. 231 et s. ; C. de Terwangne, « Le rapport de la vie privée à l'information », *in Droit des technologies de l'information. Regards prospectifs* (dir. E. Montero), Bruxelles, Bruylant, 1999, p. 138 ; R. Leenes et B.-J. Koops, « 'Code' and privacy or how technology is slowly eroding privacy' », *in Coding regulation. Essays on the Normative Role of Information technology* (dir. E. Dommering et L. Asscher), La Haye, TMC Asser Press, 2006, pp. 143 et 144.

[281] C. de Terwangne, « Le rapport de la vie privée à l'information », *in Droit des technologies de l'information. Regards prospectifs* (dir. E. Montero), Bruxelles, Bruylant, 1999, p. 138.

c) Que penser alors de l'article 8 de la Charte des droits fondamentaux de l'Union européenne ? Comme il en sera fait état ultérieurement[282], l'article 8 de la Charte des droits fondamentaux de l'Union européenne consacre le droit à la protection des données à caractère personnel de manière autonome par rapport au droit à la protection de la vie privée consacré par l'article 7 de ladite Charte. Dorénavant, les actes de droit communautaire dérivé peuvent être confrontés directement au droit à la protection des données à caractère personnel.

Il faut reconnaître qu'une telle disposition offre la force de la clarté au droit à la protection des données à caractère personnel puisque l'article 8 de la Charte indique clairement les éléments que doit respecter un traitement des données à caractère personnel.

Néanmoins, une telle disposition est critiquable car « elle coupe la protection des données nominatives de ses racines » et risque de faire oublier « aux avocats et aux législateurs [...] l'ancrage fondamental des régimes de protection des données dans les principes de dignité et d'autonomie humaine qui sont à la base de la protection de la vie privée »[283]. En effet, rappelons que la protection des données n'est pas une valeur, mais un outil. Le fait qu'elle soit érigée au rang de norme de référence risque de rendre plus difficile encore l'appréciation de la qualité d'une norme relative à la protection des données à caractère personnel, étant donné qu'on ne peut plus se référer à une valeur en fonction de laquelle on apprécierait l'équilibre à instaurer entre le responsable du traitement et la personne concernée. Du même coup, il devient plus difficile d'adapter ces normes aux nouveaux défis technologiques[284].

II. La protection des données à caractère personnel : un régime juridique spécifique

65.- Un régime juridique composé de normes diverses. Bien que fondé sur le droit à la protection de la vie privée, le régime juridique de la protection des données à caractère personnel est composé de normes visant spécifiquement à garantir la protection des données à caractère personnel. Celles-ci émanent d'instances supranationales et nationales. Les

[282] *Voy. infra* n°s 59 et s.

[283] E. Degrave et Y. Poullet, « Le droit au respect de la vie privée face aux nouvelles technologies », *in Les droits constitutionnels en Belgique* (dir. M. Verdussen et N. Bonbled), Bruxelles, Bruylant, 2011, pp. 1010 et 1011.

[284] Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *op. cit.*, pp. 168 et 169.

lignes qui suivent en dressent le panorama général, sans entrer dans le contenu de ces normes[285].

66.- La Convention n° 108 du Conseil de l'Europe. La Convention du Conseil de l'Europe n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard des traitements automatisé des données à caractère personnel[286] est le premier instrument international juridiquement contraignant en matière de protection des données à caractère personnel. Il fixe les principes à respecter en cette matière, qui seront ensuite précisés par les normes européennes et nationales.

Cet accord a une vocation universelle, et non seulement européenne, étant ouvert à l'adhésion de tous les États, qu'ils soient ou non, membres de l'Union européenne. C'est d'ailleurs la raison pour laquelle il est dénommé « Convention » et non « Convention européenne »[287].

La Belgique a signé cette Convention le 7 mai 1982. À l'époque, elle ne pouvait cependant pas encore la ratifier. En effet, l'article 4 de la Convention prévoit que « chaque Partie prend, en son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données [...] ». Cette exigence s'explique par la volonté des auteurs de la Convention de faire coïncider la date d'entrée en vigueur de la Convention sur le territoire d'un État, avec celle des mesures adoptées en droit interne[288]. Concrètement, tant que la ratification de cette Convention n'était pas effectuée, les citoyens ne pouvaient revendiquer aucun droit en se fondant directement sur celle-ci car elle n'a pas de caractère « self-executing »[289].

---

[285] Le contenu des normes fait l'objet d'amples précisions tout au long des développements qui constituent les trois titres de la recherche.

[286] Ci-après « Convention n° 108 ». Cette Convention a été ouverte à la signature des États le 28 janvier 1981, mais n'est entrée en vigueur que le 1er octobre 1985. En vertu de l'article 22 de la Convention n° 108, celle-ci entre en vigueur « le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq États membres du Conseil de l'Europe auront exprimé leur consentement à être liés par la Convention », par la ratification, l'acceptation ou l'approbation. Les cinq premiers États à avoir ratifié la Convention sont la Suède (le 29 septembre 1982), la France (le 24 mars 1983), la Norvège (le 20 février 1984), l'Espagne (le 31 janvier 1984) et l'Allemagne (le 19 juin 1985).

[287] Convention n° 108, *Rapport explicatif*, § 24.

[288] *Ibid.*, § 39.

[289] *Ibid.*, § 38. Le législateur belge a toutefois affirmé jadis qu'on ne « pourrait empêcher qu'un juge confère un effet direct à l'une ou l'autre disposition » et que « le citoyen qui s'estime lésé aux termes de cette Convention, [pourrait] introduire une demande en réparation auprès de la juridiction civile » [Projet de loi portant approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, *Doc. Parl.*, Ch. Repr., sess. 1990-1991, n° 1312/2, p. 5].

En Belgique, les mesures donnant effet à la Convention n° 108 ont été organisées par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. C'est pourquoi, la ratification belge de la Convention n° 108 a tardé et n'a pu être effectuée que le 28 mai 1993[290].

67.- La directive européenne 95/46/CE et l'article 8 de la Charte des droits fondamentaux. La protection des données à caractère personnel est encadrée par deux instruments européens. Il s'agit, d'une part, de la directive du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[291]. Il s'agit, d'autre part, de l'article 8 de la Charte des droits fondamentaux de l'Union européenne[292].

a) La directive 95/46/CE. Elle précise et amplifie les principes contenus dans la Convention n° 108[293]. L'adoption de cette directive est motivée par le souci d'encourager les activités économiques au sein du marché intérieur. On souhaite assurer une protection équivalente des données à caractère personnel au sein de chaque État membre, afin de ne pas freiner la transmission de ces données d'un État à un autre, ce qui porterait atteinte à la libre circulation des personnes, des marchandises, des services et des capitaux[294].

L'harmonisation en ce domaine se justifie également au regard du processus d'intégration communautaire. En effet, « dans le contexte de l'abolition des frontières, [...] la collaboration entre les administrations nationales sont amenées à s'intensifier. [...] Dans ce contexte, la circulation des données devient une condition indispensable du processus de coopération. Ainsi, les devoirs de collaboration ou d'information qui seront imposés aux administrations par le droit communautaire nécessitent que, parallèlement, la protection des personnes à l'égard des personnes concernées soit pleinement assurée »[295].

---

[290] Loi du 17 juin 1991 portant approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, *M.B.,* 30 décembre 1993.

[291] *J.O.C.E.,* L. 281/31 du 23 novembre 1995. Ci-après « Directive 95/46/CE ».

[292] Ci-après, « la Charte ».

[293] Considérant 11 de la directive 95/46/CE.

[294] Voy. en particulier les considérants 3, 7 et 8 de la Directive 95/46/CE.

[295] Proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement de données à caractère personnel, Exposé des motifs, COM(90) 314 final –SYN 287 et 288, 13 septembre 1990, p. 16.

Enfin, signalons que la directive 95/46/CE connaîtra prochainement une profonde réforme. En effet une proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est actuellement en cours de discussion[296]. Dans toute la mesure du possible, il y sera fait référence dans le cadre de la présente recherche.

b) L'article 8 de la Charte. Le 7 décembre 2000 a été adoptée la *Charte des droits fondamentaux de l'Union européenne*[297]. Celle-ci consacre, en son article 8, le droit à la protection des données à caractère personnel, distinct du droit à la protection de la vie privée consacré par l'article 7 de ladite Charte.

La rédaction de cette disposition s'inspire directement de la Convention n° 108 et de la directive 95/46/CE.

> L'article 8 de la Charte des doits fondamentaux de l'Union européenne est formulé comme suit :
>
> « Toute personne a droit à la protection des données à caractère personnel la concernant.
>
> Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
>
> Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Depuis l'entrée en vigueur du Traité de Lisbonne le 1er décembre 2009, l'article 8 de la Charte jouit d'une force juridique contraignante en vertu de l'article 6 du Traité de l'Union européenne[298]. Il ne s'agit guère d'une révolution dans la protection des droits fondamentaux au sein de l'Union, mais plutôt d'une avancée symbolique étant donné que la Charte « a été conçue comme devant constituer une codification de l'acquis existant de l'Union européenne, plutôt que comme la proclamation de droits nouveaux »[299].

---

[296] SEC (2012) 72 final.

[297] Ci-après, « la Charte ».

[298] Voy. C.J.U.E., gde ch., 9 novembre 2010, *Volker und Markus Schecke GbR* et *Hartmut Eifert,* aff. jtes C-92/09 et C-93/09. Pour un commentaire de cet arrêt voy. E. Degrave, « Arrêt 'Volker und Markus Schecke et Eifert': le droit fondamental à la protection des données à caractère personnel et la transparence administrative », *J.D.E.,* 2011, pp. 97 à 99.

[299] O. De Schutter, « Les droits fondamentaux dans l'Union européenne (1er janvier 2007- 1er février 2008)», *J.D.E.,* 2008, p. 126.

Concrètement, les actes de droit communautaire dérivé peuvent désormais être confrontés directement au droit à la protection des données à caractère personnel, sans devoir démontrer une atteinte à la protection de la vie privée. C'est ce qu'a fait récemment la Cour de justice de l'Union européenne.

Dans son arrêt du 9 novembre 2010[300], la Cour invalide partiellement une réglementation européenne qui, par souci de transparence, imposait la publication, sur Internet, du nom et de la localité des agriculteurs ayant bénéficié de subsides européens. C'est la première fois que la Cour se fonde sur le droit à la protection des données à caractère personnel, consacré par l'article 8 de la Charte, afin d'invalider un acte de droit communautaire dérivé.

Néanmoins, elle insiste sur les liens qui unissent l'article 8 de la Charte et l'article 7 de celle-ci, qui consacre le droit à la protection de la vie privée. Elle rappelle également que les articles 52, §3, et 53 de la Charte imposent explicitement au juge de se référer à l'interprétation que donne la Cour européenne des droits de l'homme du contenu de ces droits et des limites qui peuvent leur être apportées[301].

68.- La loi belge du 8 décembre 1992, les lois sectorielles, les normes des entités fédérées. Le corpus normatif belge est complexe. Il se compose d'une loi générale- la loi du 8 décembre 1992 relative à la protection

[300] C.J.U.E., gde ch., 9 novembre 2010, *Volker und Markus Schecke GbR* et *Hartmut Eifert,* précité. Pour un commentaire de cet arrêt voy. E. DEGRAVE, « Arrêt 'Volker und Markus Schecke et Eifert' : le droit fondamental à la protection des données à caractère personnel et la transparence administrative », *op. cit.*, pp. 97 à 99.

[301] En toute rigueur, cette affirmation doit être quelque peu nuancée au regard des explications de la Charte, établies sous la responsabilité du Praesidium de la Convention européenne et destinées à éclairer l'interprétation des dispositions de la Charte (CHARTE 4487/00 CONVENT 50, du 19octobre 2000. Les explications de la Charte ont été mises à jour en 2003 : CONV 828/03 du 9 juillet 2003). En effet, les explications relatives à l'article 52 de la Charte ne mentionnent pas l'article 8 parmi les droits « correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales » dont le sens et la portée « sont les mêmes que ceux que leur confère ladite convention ». Néanmoins, cela ne signifie pas que la riche jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8 de la Convention européenne des droits de l'homme consacrant le droit à la protection de la vie privée ne puisse être appliqué à l'article 8 de la Charte. En effet, une telle exclusion serait contraire à la « clause de protection » prévue à l'article 53 applicable à l'article 8 de la Charte. Voy. O. DE SCHUTTER, « Article II-68 », *in Traité établissant une Constitution pour l'Europe. Partie II, La Charte des droits fondamentaux de l'Union. Commentaire article par article.* (dir. L. BURGORGUE-LARSEN, A. LEVADE et F. PICOD), T. 2, Bruxelles, Bruylant, 2005, pp. 123-124 ; B. FAVREAU, « La protection des données à caractère personnel », *in La Charte des droits fondamentaux de l'Union européenne après le Traité de Lisbonne* (dir. B. FAVREAU), Bruxelles, Bruylant, 2010, p. 196.

de la vie privée à l'égard des traitements de données à caractère personnel[302] – ainsi que de lois particulières, appelées aussi « lois sectorielles », et de normes émanant des entités fédérées.

a) La loi du 8 décembre 1992. La loi du 8 décembre 1992 s'applique à tous les traitements de données[303], qu'ils soient effectués dans le secteur public ou le secteur privé. Elle a été adoptée pour donner effet, en droit belge, à la Convention n° 108. Elle était attendue depuis plusieurs années. Ce sont les discussions parlementaires entourant la mise en place du premier outil phare de l'e-gouvernement, à savoir, le Registre national, en 1983, qui ont fait apparaître l'importance de veiller à la protection de la vie privée des citoyens face aux développements technologiques[304].

Quelques années après son adoption, la loi du 8 décembre 1992 a été profondément modifiée par la loi du 11 décembre 1998, afin d'être mise en conformité avec la directive 95/46/CE adoptée entre temps[305].

La loi du 8 décembre est exécutée par l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[306]. Cet arrêté royal organise notamment l'obligation de déclarer les traitements de données ainsi que le Registre public des traitements de données à caractère personnel. Il prévoit également d'importantes exceptions en matière de transparence, au bénéfice des administrations. Nous y reviendrons plus en détails ultérieurement[307].

D'autres normes de valeur réglementaire complètent encore l'arsenal normatif fédéral et feront l'objet de réflexions dans cette recherche, tel que l'arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP[308].

b) Les lois sectorielles. Le régime juridique belge de la protection des données ne se réduit pas à la loi du 8 décembre 1992. Des règles de

---

[302] *M.B.,* 18 mars 1993. Ci-après « la loi du 8 décembre 1992 ».

[303] Art. 3, al. 1er, de la loi du 8 décembre 1992.

[304] Voy. not. le Rapport fait au nom de la Commission de l'Intérieur, des Affaires générales et de la Fonction publique concernant la loi organisant un registre national des personnes physique, par M. Tant, *Doc. Parl.,* Ch. Repr., session 1982-1983, n° 513/6 du 12 juin 1983, p. 1350.

[305] Loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.,* 3 février 1999.

[306] *M.B.,* 13 mars 2001.

[307] En particulier dans le Titre II relatif à la transparence de l'e-gouvernement.

[308] *M.B.,* 30 décembre 2003.

protection des données sont également prévues par des lois particulières, qu'on appelle « lois sectorielles »[309]. Celles-ci sont de plus en plus nombreuses. Elles mettent en place un outil de traitement de données particulier, et prévoient, ci et là, des règles relatives à la protection de la vie privée des personnes concernées par celui-ci.

Dans le cadre de cette étude consacrée à l'e-gouvernement, nous nous concentrons principalement sur la loi du 8 août 1983 organisant un registre national des personnes physiques[310] et la loi du 15 janvier 1991 sur la Banque-Carrefour de la sécurité sociale[311] qui sont antérieures à la loi du 8 décembre 1992. D'autres lois plus récentes retiennent également notre attention, comme la loi du 16 janvier 2003 sur la Banque-Carrefour des entreprises[312], la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules[313] ou encore la loi du 14 avril 2011 portant des dispositions diverses qui institue la Banque-Carrefour des permis de conduire[314].

c) Les normes des entités fédérées. À ces lois sectorielles s'ajoutent des normes adoptées par les autorités fédérées. On pense notamment au décret flamand du 18 juillet 2008 relatif à l'échange de données administratives[315] qui organise, comme son nom l'indique, l'échange des données entre les administrations flamandes. La Communauté française et la Région wallonne ont récemment suivi la même voie en adoptant un accord de coopération régissant le partage de données entre ces deux entités[316].

---

[309] Ce terme est utilisé par la directive 95/46/CE qui prévoit, en son considérant 23, que « les États membres sont habilités à assurer la mise en œuvre de la protection des personnes, tant par une loi générale relative à la protection des personnes à l'égard du traitement des données à caractère personnel que par des lois sectorielles telles que celles relatives par exemple aux instituts de statistiques ».

[310] Loi du 8 août 1983 sur le Registre national.

[311] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.,* 22 février 1990.

[312] Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre du commerce, création de guichets-entreprises agréés et portant diverses dispositions, *M.B.*, 5 février 2003.

[313] Loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules, *M.B.*, 28 juin 2010.

[314] Loi du 14 avril 2011 portant des dispositions diverses, *M.B.,* 6 mai 2011.

[315] Decreet betreffende het elektronische bestuurlijke gegevensverkeer, *M.B.,* 29 octobre 2008.

[316] Accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.,* 23 juillet 2013.

Section 2. Les notions cardinales de la protection des données à caractère personnel

69.- Considérations générales. Il convient à présent de définir trois éléments importants de la protection des données, car ils reviendront à maintes reprises dans la suite de cette recherche. Il s'agit des notions de « donnée à caractère personnel », de « traitement de données », et de « responsable du traitement ».

I. La donnée à caractère personnel

70.- La définition. Tant la Convention n° 108, que la directive 95/46/CE et la loi du 8 décembre 1992 définissent la « donnée à caractère personnel » comme « toute information concernant une personne physique identifiée ou identifiable »[317].

71.- Le caractère identifiable de la personne. Comme l'indique la définition précitée, dès le moment où l'information concerne une personne « identifiable », son utilisation est soumise aux règles de protection des données.

La directive 95/46/CE et la loi du 8 décembre 1992 précisent qu'est réputée identifiable « une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

Pour le dire autrement, dès le moment où l'information peut être rattachée à une personne physique, il s'agit d'une donnée à caractère personnel, peu importe que ce rattachement soit effectué par le responsable du traitement ou une autre personne[318]. Il faut donc apprécier le caractère identifiable de la personne *in abstracto,* et non par rapport aux moyens dont le responsable du traitement dispose *in concreto*[319].

Ainsi, comme l'exprime l'exposé des motifs de la loi du 11 décembre 1998 qui a transposé, dans l'ordre juridique belge, la directive 95/46/CE,

[317] Art. 2, a), de la Convention n° 108 ; art. 2, a), de la directive 95/46/CE ; art. 1er, §1er, de la loi du 8 décembre 1992.

[318] Considérant 26 de la directive 95/46 ; H. Graux et J. Dumortier, *Privacywetgeving in de praktijk,* Courtrai, UGA, 2009, pp. 22 et 32.

[319] C. de Terwangne, « La nouvelle loi belge de protection des données à caractère personnel », *in Cahiers de sciences morales et politiques,* 2002, p. 92.

« une information relative à une personne est donc considérée comme donnée à caractère personnel tant que quelqu'un est encore en mesure, par quelque moyen qui puisse raisonnablement être mis en œuvre, de déterminer à quel individu se rapporte cette information. Sont donc également considérées comme 'données à caractère personnel' les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne. Lorsque les informations relatives à des personnes physiques sont rendues anonymes, elles ne perdent donc leur caractère de données à caractère personnel que si le caractère anonyme est absolu et que plus aucun moyen raisonnablement susceptible d'être mis en œuvre ne permet de revenir en arrière pour briser l'anonymat »[320].

72.- Des exemples. Les données les plus diverses peuvent être qualifiées de données à caractère personnel, dès le moment où elles concernent une personne identifiée ou identifiable.

Par exemple, le numéro d'identification au Registre national de chaque citoyen est une donnée à caractère personnel. L'administration qui traite cette information est tenue de respecter les règles de protection des données, et ce, même dans l'hypothèse où elle n'aurait pas elle-même accès au Registre national et ne pouvait donc elle-même faire le lien entre ce numéro d'identification et la personne physique concernée.

Il en va de même d'un numéro de plaque d'immatriculation, d'un numéro de compte bancaire, des photos, des données codées regroupées dans un entrepôt de données, etc.

II. Le traitement de données

73.- La définition. Les règles de protection des données ne s'appliquent que si les données à caractère personnel sont soumises à un « traitement ».

Ce terme désigne « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute

[320] Exposé des motifs précédant le projet de loi transposant la Directive 95/46/CE du 24 octobre 1995du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Doc. Parl.,* Ch. Repr., session 1997-1998, n° 1566/1, p. 12.

autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »[321].

74.- Moyens automatisés ou fichiers. Il faut comprendre par là que toute opération qui en appelle à des moyens automatisés, ne fût-ce qu'en partie, est un traitement de données soumis aux règles de protection des données[322].

> Ce peut être le cas, par exemple, de données à caractère personnel envoyées par mail, mais également par fax, sur un cd-rom, une clé USB, etc.
>
> Faire apparaître des données sur un site internet implique également l'utilisation de moyens automatisés, notamment lors du chargement des informations sur un serveur et de leur mise en ligne sur internet afin de les rendre accessibles au public[323].

Les règles de protection des données s'appliquent également aux opérations non automatisées, si elles impliquent l'utilisation de données contenues dans un fichier[324], c'est-à-dire, « un ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »[325].

> Ne répond pas à la notion de « fichier », un dossier qui contient un ensemble de feuilles isolées, non classées selon un critère déterminé tel qu'un ordre alphabétique. Dès lors, la consultation de ces papiers, ou leur envoi par courrier postal ne sont pas des opérations soumises aux règles de protection des données[326].

---

[321] Art. 2, b), de la directive 95/46 ; art. 1er, § 2, de la loi du 8 décembre 1992. La Convention n° 108, en son art. 2, c), contient une définition du « traitement automatisé » qui s'inscrit dans le même sens que celle de la directive 95/46 et de la loi du 8 décembre 1992 tout en étant plus sommaire qui prévoit qu'un « traitement automatisé » s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion.

[322] Art. 3, § 1er, de la Convention n° 108 ; art. 3, § 1er, de la directive 95/46/CE ; art. 3, § 1er, de la loi du 8 décembre 1992 ; J. Dumortier et F. Robben, « Inleiding », *in Persoonsgegevens en privacybeescherming. Commentaar op de wet tot bescherming van de persoonlijke levensfeer* (dir. J. Dumortier et F. Robben), Brugge, die Keure, 1995, p. 31.

[323] En ce sens, voy. C.J.U.E., 6 novembre 2003, *Bodil Linqvist c. Suède,* C-101/01, § 26.

[324] Art. 3, § 1er, de la Convention n° 108 ; art. 3, § 1er, de la directive 95/46/CE ; art. 3, § 1er, de la loi du 8 décembre 1992.

[325] Art. 2, c), de la Directive 95/46/CE ; art. 11er, § 3, de la loi du 8 décembre 1992.

[326] En ce sens, voy. C. de Terwangne, « La nouvelle loi belge de protection des données à caractère personnel », *op. cit,* p. 94 et références citées ; L. Moes, « Passieve openbaarheid van bestuur en privacybescherming », *in Het handvest van de sociaal verzekerde en bestuurlijke vernieuwing in de sociale zekerheid* (dir. J. Put), Brugge, die Keure, 1999, p. 230.

III. Le responsable du traitement

75.- Un rôle central. Comme son nom le laisse penser, le responsable du traitement joue un rôle central dans l'application du régime juridique de la protection des données à caractère personnel, puisqu'il est chargé de faire respecter ces règles. C'est à lui que revient notamment le soin de veiller à ce que les personnes concernées puissent accéder à leurs données.

Il importe, dès lors, d'identifier le responsable du traitement au sein de chaque administration qui traite des données.

> La directive 95/46/CE dispose que le responsable du traitement est, notamment[327], « l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou règlementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire »[328].
>
> La loi du 8 décembre 1992 prévoit qu'est responsable du traitement, « l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est [...] l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance »[329].

Lorsque l'on cherche à identifier qui est responsable du traitement dans l'administration, les normes précitées prêtent à confusion. Elles permettent difficilement de savoir quelle norme doit déterminer le responsable de traitement et qui peut revêtir cette qualité. Les lignes qui suivent entendent éclairer cette problématique.

76.- Une désignation par la loi. Comme le souligne le premier titre de la recherche[330], en vertu de l'article 22 de la Constitution qui impose que toute immixtion dans la vie privée soit organisée par une loi prévisible, il revient au législateur de désigner explicitement le responsable du traitement dans la loi qui organise le traitement de données. De l'avis de la CPVP, « la désignation du responsable du traitement est essentielle.

---

[327] Nous ne traitons que des hypothèses liées à l'administration.
[328] Art. 2, d), de la Directive 95/46/CE.
[329] Art. 1, § 4, de la loi du 8 décembre 1992.
[330] Voy. *infra*, n°s 78.- et s.

Celle-ci a des répercussions concrètes au niveau du respect des droits et obligations en vertu de la [loi du 8 décembre 1992] comme le droit à l'information [...]. L'obligation de désigner le responsable dans la loi découle [...] de la nécessité d'une 'loi accessible et prévisible' »[331].

Remarquons que la loi du 8 décembre 1992 peut induire en erreur en disposant que « lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est [...] l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance »[332]. Les termes « en vertu de » laissent entendre que le responsable du traitement pourrait être désigné dans une norme de valeur réglementaire. L'analyse de la jurisprudence de la Cour constitutionnelle relative à l'article 22 de la Constitution montre pourtant que la détermination d'un élément si essentiel du traitement porterait atteinte à la prévisibilité du traitement de données à caractère personnel[333].

Le législateur doit effectuer cette désignation en tenant compte de la réalité. Il est ainsi tenu de désigner, comme responsable du traitement, l'administration qui a les traitements de données dans ses compétences légales et qui, de ce fait, exerce une véritable maîtrise sur ceux-ci[334]. L'organe consultatif européen sur la protection des données et la vie privée, dit « Groupe 29 », s'est d'ailleurs récemment prononcé dans le même sens en soutenant qu' « une désignation officielle par la loi n'en doit pas moins être conforme aux règles de protection des données, en veillant à ce que l'organisme désigné ait un contrôle effectif sur les opérations de traitement ou, en d'autres termes, que la désignation par la loi reflète la réalité de la situation »[335].

Cela signifie qu'au sein d'un réseau sectoriel, chaque administration qui détient une source authentique fournissant des données à ce réseau doit être désignée comme responsable du traitement des données qu'elle gère[336]. Plus encore, si, au sein d'une même administration, différents services gèrent des traitements de données répondant à des finalités

[331] CPVP, avis n° 23/2008 du 11 juin 2008 relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules, p. 18, n° 49. À ce sujet, la CPVP s'était prononcée dans le même sens précédemment. Voy. avis n° 42/2006 du 18 octobre 2006 concernant l'avant-projet de loi portant création d'une source authentique relatives aux véhicules, p. 4, n° 11.

[332] Art. 1, § 4, de la loi du 8 décembre 1992.

[333] Voy. *infra*, n°s 99.- et s.

[334] CPVP, avis n° 15/2000 du 24 mai 2000 relatif à un projet de décret du gouvernement régional wallon relatif aux archives publiques, p. 5, n° 13.

[335] Groupe 29, avis 1/2010 sur les notions de 'responsable du traitement' et de « 'sous-traitant' », du 16 février 2010, WP 169, p. 13.

[336] CPVP, avis n° 23/2008, *op. cit.*, pp. 16 et 17, n°s 43 et 44.

différentes, il y a lieu d'attribuer à chacun de ces services la qualité de responsable du traitement[337].

Par ailleurs, il est conseillé au législateur de désigner, comme responsable du traitement, un organisme plutôt qu'une personne en son sein. De cette manière, les personnes concernées peuvent « s'adresser à une entité plus stable et plus fiable lorsqu'elles exercent [leurs] droits »[338]. Cela n'empêche que chaque administration peut utilement désigner une personne en particulier pour être le point de contact des citoyens.

> Le législateur l'a déjà fait à plusieurs reprises. Ainsi, l'article 7 de la loi du 14 avril 2011 portant des dispositions diverses[339] prévoit que le responsable du traitement des données à caractère personnel figurant dans la Banque-Carrefour des permis de conduire est le service de gestion, à savoir la Direction générale Mobilité et Sécurité routière du Service public fédéral Mobilité et Transports. Dans le même sens, l'article 2 de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions[340] affirme que le responsable du traitement est le Service public fédéral Finances.

77.- Et si la loi ne désigne par le responsable du traitement ? Nombre de lois régissant actuellement un pan de l'e-gouvernement ne désignent pas explicitement le responsable du traitement. Bien que cette lacune menace la prévisibilité de la loi organisant ledit traitement, il n'en demeure pas moins qu'un responsable du traitement doit, de fait, pouvoir être identifié, au risque de priver les citoyens de l'exercice effectif de leurs droits.

Dans une telle hypothèse, on considère que le responsable du traitement est l'administration qui exerce la maîtrise sur le traitement, c'est-à-dire, celle dont les compétences légales comprennent les finalités du traitement en cause[341].

> Par exemple, la CPVP considère que, même si la loi est silencieuse sur ce point, la Banque-Carrefour de la sécurité sociale est le responsable du traitement des données qui circulent dans le réseau de la sécurité sociale[342].

---

[337] CPVP, avis n° 01/2007 du 17 janvier 2007 concernant un avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances, p. 5, n° 20. La Commission a considéré que les trois grandes directions générales du SPF Finances réalisent des traitements « bien distincts » et doivent, de ce fait, revêtir chacun la qualité de responsable de leurs traitements.

[338] Groupe 29, avis 1/2010, *op. cit.*, p. 16.

[339] *M.B.*, 6 mai 2011.

[340] *M.B.*, 24 août 2012.

[341] En ce sens, CPVP, avis n° 23/2008, *op. cit.*, p. 18, n° 51.

[342] CPVP, avis n° 14/2005 du 28 septembre 2005 faisant suite à une décision d'évocation dans les dossiers SCSZ/05/70, SCSZ/05/90, SCSZ/05/110 et SCSZ/05/113 transmise par le Président du Comité sectoriel de la Sécurité sociale, p. 9, n° 10.5.

Cette responsabilité implique notamment que la Banque-Carrefour « doit toujours veiller à ce que l'on utilise les données correctes et actuelles, [...] que l'on consulte toujours la bonne source authentique lors de la prise de décisions, et ce en plus de chaque enregistrement interne de ces données »[343]. Néanmoins, étant donné que ces données émanent de sources authentiques instituées sous la responsabilité d'autres institutions, la CPVP soutient qu'« il peut être question d'une coresponsabilité en vertu de la [loi du 8 décembre 1992] »[344].

*

Conclusions

Les règles de protection des données forment un régime juridique spécifique, organisé par des règles supranationales – la Convention n° 108, la directive 95/46/CE et l'article 8 de la Charte des droits fondamentaux – ainsi que des règles nationales, contenues dans la loi du 8 décembre 1992 et des normes particulières.

La protection ainsi mise en œuvre est large. Elle s'applique à tout traitement de données concernant une personne identifiable et peut être opposée à chaque responsable de traitement. Ces notions importantes ont été définies et illustrées.

Dans l'e-gouvernement, les règles de protection des données permettent au citoyen de faire valoir certains droits auprès de l'administration qui traite ses données. Il peut ainsi, notamment, accéder aux données conservées et connaître l'usage qui en sera fait. Ce faisant, chaque personne garde la maîtrise de ses informations personnelles, ce qui est important dans le contexte de l'e-gouvernement qui génère le risque d'un déséquilibre entre une administration puissante et des citoyens vulnérables.

Même si elle répond également à d'autres droits fondamentaux, la protection des données s'enracine dans le droit fondamental à la protection de la vie privée. Ce droit fondamental est riche et protège aussi bien la solitude, que l'interaction avec autrui. Ces deux facettes de la vie privée nourrissent les règles de protection de données et les guident dans le souci de protéger le libre épanouissement personnel de chacun.

*

[343] CPVP, avis n° 14/2010 du 31 mars 2010 relatif à un avant-projet de loi portant création de la Banque-Carrefour des permis de conduire, p. 6, n° 18.

[344] *Idem.*

Conclusions du prélude

Au terme de ce prélude, les contours de l'e-gouvernement sont délimités. Ils laissent apparaître les nombreuses potentialités des outils de traitements de données à disposition des administrations. Ainsi, les sources authentiques de données, les plateformes d'échanges d'informations et les numéros d'identification permettent de réaliser le principe de la collecte unique des données et de mettre en œuvre des nouvelles opérations, au bénéfice tant de l'administration que des citoyens. Si ce constat génère de l'enthousiasme à l'idée que l'efficacité administrative puisse être renforcée, il incite également à la prudence car l'utilisation des technologies dans l'administration provoque à maints égards des bouleversements.

Face à de telles craintes, le régime juridique de la protection des données à caractère personnel offre ses plus belles promesses. Enraciné dans la protection de la vie privée, il balise les traitements de données à caractère personnel de manière à garantir à chacun les conditions pour s'épanouir librement, entre le besoin de solitude et la nécessité d'entretenir des relations avec autrui.

Néanmoins, le régime juridique de la protection de la vie privée est-il suffisamment adapté à l'e-gouvernement ? La question mérite une attention particulière en constatant que les craintes mises en évidence dans le premier chapitre sont actuelles. Or, les règles de protection des données existent depuis plusieurs années. On en déduit donc que ces règles ne permettent pas, pour le moment, de répondre à tous les dangers de l'e-gouvernement.

C'est pourquoi, les développements qui suivent révèlent notamment les faiblesses des règles de protection des données lorsqu'elles sont appliquées à l'e-gouvernement et envisagent des solutions pour garantir pleinement la protection de la vie privée des citoyens dans ce contexte administratif nouveau.

* * *

Titre I.
La légalité de l'e-gouvernement

Introduction

D'emblée, il est frappant de constater que l'e-gouvernement est encadré par des règles nombreuses, éparses, difficiles à comprendre, qui émanent du pouvoir législatif et du pouvoir exécutif, de la collectivité fédérale et des collectivités fédérées. Dans un tel contexte, peut-on considérer que l'encadrement législatif des traitements de données effectués dans l'administration répond adéquatement au souci de protéger la vie privée des citoyens ?

Cette question est particulièrement importante s'agissant des données personnelles détenues par l'administration. Ainsi qu'on l'a dit[345], dans ses relations avec l'administration, le citoyen ne peut pas choisir de communiquer, ou non, ses informations personnelles. Il est contraint de le faire. Il est ainsi privé du « droit fondamental susceptible de garantir la protection de [sa] vie privée sur le plan de la circulation des données, c'est-à-dire, le droit de ne pas autoriser son enregistrement dans un fichier »[346]. De plus, les informations qui lui sont demandées sont nombreuses et touchent à des sphères diverses de sa vie privée.

Il importe dès lors d'encadrer minutieusement l'usage que l'administration peut faire de cette masse d'informations. Il en va d'autant plus ainsi que les progrès techniques sont tentants. Comme dit précédemment[347], les technologies mises à disposition de l'administration augmentent le risque que l'individu perde la maîtrise de ses propres données. Réfléchir à l'encadrement législatif de l'e-gouvernement suppose de revenir aux fondements juridiques qui justifient l'intervention du législateur en ce domaine.

Ces règles sont de deux ordres. Les premières règles émanent de la Constitution. En vertu de l'article 105 de la Constitution, l'administration n'a d'autres pouvoirs que ceux que lui attribuent la Constitution et les lois particulières portées en vertu de celle-ci. Par ailleurs, l'article 22 de la Constitution protège le droit à la protection de la vie privée et requiert du législateur qu'il organise chaque ingérence dans ce droit fondamental. Les secondes règles sont issues de normes supranationales. Ainsi, l'article 8 de

[345] Voy. *supra,* n° 62.-

[346] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la Commission de la Justice par M. Vandenberghe, *Doc. Parl.,* Ch. Repr., session extr. 1991-1992, n° 445/2, p. 43.

[347] Voy. *supra,* n° 49.-

la Convention européenne des droits de l'homme et la directive 95/46[348] fixent des impératifs dont le législateur doit également tenir compte.

Cette première partie de la recherche entend donc examiner la manière dont ces deux corps de règles peuvent être combinés. Le but de cette analyse est de dégager une méthode qui permet au législateur d'encadrer adéquatement l'e-gouvernement. C'est l'objet des deux premiers chapitres. Fort de ces enseignements, le troisième chapitre propose un modèle d'e-gouvernement qui garantisse la protection de la vie privée des citoyens tout en assurant l'efficacité de l'administration.

* * *

[348] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ci-après « directive 95/46 ». À ce sujet, voy. *supra,* n° 67.-

CHAPITRE I.
L'e-gouvernement et l'exigence constitutionnelle de légalité

Introduction

78.- L'exigence constitutionnelle de légalité. L'e-gouvernement est soumis à une exigence de légalité fondée sur les articles 105 et 22 de la Constitution. Comme le souligne l'introduction, cette exigence de légalité impose à l'administration de se soumettre aux règles de droit dans l'exercice de ses missions.

a) L'article 105 de la Constitution. L'e-gouvernement concerne la structure et le fonctionnement de l'administration. C'est pourquoi, l'e-gouvernement doit respecter l'exigence de légalité entendue au sens formel du terme, consacrée par l'article 105 de la Constitution.

> L'article 105 de la Constitution affirme que « le Roi n'a d'autres pouvoirs que ceux que lui attribuent formellement la Constitution et les lois particulières portées en vertu de la Constitution même ».

En d'autres termes, tout acte du Roi, et, de manière générale, du pouvoir exécutif, doit se fonder sur des règles émanant d'une autorité supérieure, le Constituant ou, à défaut, le législateur[349].

b) L'article 22 de la Constitution. Puisqu'il implique des traitements de données à caractère personnel considérés comme des ingérences dans la protection de la vie privée des citoyens[350], l'e-gouvernement est

[349] Art. 105 de la Constitution ; F. Delpérée, *Le droit constitutionnel de la Belgique*, Bruxelles, Bruylant, Paris, L.G.D.J., 2000, p. 91 ; M. Uyttendaele, *Précis de droit constitutionnel belge : Regards sur un système institutionnel paradoxal*, Bruxelles, Bruylant, 2005, 3e éd., p. 149 ; H. Simonart, « L'article 105 », *in La Constitution. Lignes & entrelignes* (dir. M. Verdussen), Bruxelles, Le Cri, 2004, pp. 247-249 ; A. Mast, J. Dujardin, M. Van Damme et J. vande Lanotte, *Overzicht van het Belgisch Administratief Recht,* 18e éd., Malines, Kluwer, 2009, p. 19 ; P. Goffaux, *Dictionnaire élémentaire de droit administratif,* Bruxelles, Bruylant, 2006, p. 147 ; A. Alen, *Rechter en bestuur in het Belgische publiekrecht. De grondslagen van de rechterlijke wettigsheidscontrole*, Anvers, Kluwer, 1984, t. I, pp. 1-8 ; S. Lust, *Rechtsbescherming tegen de (administratieve) overheid. Een inleiding,* Brugge, die Keure, 2010, pp. 13-14.

[350] Voy. *supra,* nos 59.- et s.

également soumis à l'article 22 de la Constitution qui prévoit une exigence de légalité plus sévère que la précédente. Nous y reviendrons.

> En vertu de l'article 22 de la Constitution, « chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.
>
> La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

L'article 22 de la Constitution est la traduction, dans l'ordre juridique belge, de l'article 8 de la Convention européenne des droits de l'homme.

> L'article 8 de la Convention européenne des droits de l'homme prévoit que
>
> « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

À maintes reprises, lors des discussions parlementaires qui ont précédé l'adoption de l'article 22 de la Constitution, on a mis en évidence la filiation entre cette disposition et l'article 8 de la Convention européenne des droits de l'homme.

> Ainsi le Constituant affirme-t-il qu'on a « cherché à mettre le plus possible la proposition en concordance avec l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), afin d'éviter toute contestation sur le contenu respectif de l'article de la Constitution et de l'article 8 de la CEDH »[351].

Depuis lors, la Cour constitutionnelle[352] ne manque pas de le rappeler et de se référer à la jurisprudence de la Cour européenne des droits de

[351] Rapport fait au nom de la Commission de la révision de la Constitution, des réformes institutionnelles et du règlement des conflits, à propos de la révision du titre II de la Constitution en vue d'y insérer un article 24*quater* relatif au respect de la vie privée, *Doc. Parl.,* Ch. Repr., session 1992-1993, n° 997/5, p. 2.

[352] La compétence de la Cour constitutionnelle est rappelée au Titre III de la présente recherche. Voy. *infra,* n°s 434.- et s.

l'homme lorsqu'elle se prononce sur une norme organisant un traitement de donnés à caractère personnel[353].

79.- Une matière embroussaillée. Ce chapitre se concentre sur l'exigence de légalité organisée par l'article 22 de la Constitution et la question de savoir si l'e-gouvernement respecte l'exigence de légalité imposée par cette disposition constitutionnelle.

On se heurte rapidement à un constat flagrant : l'e-gouvernement est encadré par des normes éparses et difficilement compréhensibles. Certains outils échappent même à tout encadrement législatif. On constate ainsi que certains aspects de l'e-gouvernement sont encadrés par des normes de valeur législative, tandis que d'autres le sont par des normes de valeur règlementaire. Certains développements de l'e-gouvernement se font même en dehors de tout encadrement normatif. On constate également que, parmi les normes de valeur législative, certaines émanent du législateur fédéral, et d'autres proviennent des communautés et des régions.

Ce constat amène à structurer nos développements en deux temps.

La première section est consacrée à l'e-gouvernement et à la répartition des compétences, dans le but de déterminer si seul le législateur fédéral est compétent pour organiser l'e-gouvernement, ou si le législateur des entités fédérées peut également intervenir dans cette matière.

La deuxième section s'attache à étudier la compétence du législateur, afin de délimiter les aspects de l'e-gouvernement qui doivent être encadrés par une loi et ceux qui peuvent être laissés au pouvoir exécutif.

*

Section 1. L'e-gouvernement et le législateur compétent

80.- Loi, décret et ordonnance ? Le législateur fédéral, les législateurs communautaires et les législateurs régionaux, sont-ils tous compétents pour organiser la protection de la vie privée dans l'e-gouvernement ? Pour le dire autrement, le mot « loi » contenu à l'article 22 de la Constitution,

[353] Voy. not. C.C., arrêt n° 162/2004, du 20 octobre 2004, B.3.1 ; C.C, arrêt n° 189/2005, du 14 décembre 2005, B. 4.3 ; C.C., arrêt n° 151/2006, du 18 octobre 2006, B. 5.4 ; C.C., arrêt n° 15/2008, du 14 février 2008, B.19.1 ; C.C., arrêt n° 29/2010, du 18 mars 2010, B.9.2.

alinéa 1er, doit-il être interprété comme la loi fédérale ou inclut-il également les décrets et les ordonnances[354] ?

> Rappelons que l'article 22, alinéa 1er, prévoit qu'une ingérence dans la protection de la vie privée des citoyens ne peut être organisée que « dans les cas et conditions fixés par la loi ».

Comme l'expliquent les lignes qui suivent, le mot « loi » inclut les lois fédérales, les décrets et les ordonnances. Néanmoins, selon la Cour constitutionnelle et la section de législation du Conseil d'État, les législateurs communautaires et régionaux doivent respecter la loi du 8 décembre 1992, ce qui est critiquable à certains égards.

I. Les décrets et les ordonnances soumis à la loi du 8 décembre 1992

81.- Plusieurs législateurs compétents. Aujourd'hui, tant le législateur fédéral, que les législateurs communautaires et régionaux, peuvent organiser des traitements de données à caractère personnel dans l'exercice de leurs compétences. C'est ce que soutient la Cour constitutionnelle, en affirmant que « la consécration, par la Constitution et les traités internationaux, de droits et libertés fondamentaux ne signifie en aucune manière que leur réglementation n'appartiendrait, en tant que telle, qu'à l'autorité fédérale. C'est à chaque autorité qu'il appartient d'en assurer le respect en les concrétisant lorsqu'elle exerce les compétences qui sont les siennes »[355].

---

[354] Les développements qui suivent sont inspirés des articles suivants : E. Degrave, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.,* 2009, pp. 365-371 ; E. Degrave et Y. Poullet, « Le droit au respect de la vie privée face aux nouvelles technologies », *in Les droits constitutionnels en Belgique* (dir. M. Verdussen et N. Bonbled), vol. 2, Bruxelles, Bruylant, 2011, pp. 1001 à 1035.

[355] C.C., arrêt n° 124/99, du 25 novembre 1999, p. 17, B.4.4. Voy. également, notamment, l'arrêt n° 124/2000 du 29 novembre 2000, p. 11, B.4.2. ; avis rendu par la section de législation du Conseil d'État le 23 mai 2002 à propos d'un avant-projet de loi portant création de l'Institut de l'égalité des femmes et des hommes, *Doc. Parl.,* Chambre, session 2001-2002, pp. 16 et 17 ; avis L. 30.462/2 à propos d'une proposition de loi tendant à lutter contre la discrimination et modifiant la loi du 15 février 1993 créant un Centre pour l'égalité des chances et la lutte contre le racisme, *Doc. Parl.,* Sénat, session 2000-2001, n° 2- 12/5, pp. 2 et 3.

Remarquons qu'il n'en a pas toujours été ainsi. Longtemps, les hautes juridictions ont considéré que seul le législateur fédéral pouvait organiser des ingérences dans le droit fondamental à la protection de la vie privée. Pour de plus amples détails à ce sujet, voy. E. Degrave, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.,* 2009, p. 365 ; J. Vande Lanotte et G. Goedertier, *Handboek Belgisch Publiekrecht,* Brugge, die Keure, 2010, pp. 126-129, n° 214 ; N. Bonbled et M. Verdussen, « Les droits constitutionnels

Les législateurs communautaires et régionaux peuvent ainsi organiser les ingérences dans la vie privée et familiale qui sont « la conséquence de la réglementation d'une matière déterminée attribuée » aux communautés et aux régions, tandis que les « restrictions générales à ce droit, applicables dans n'importe quelle matière » sont du ressort du législateur fédéral[356].

Par exemple, l'échange de données administratives dans l'administration flamande est organisé par un décret flamand[357]. La Communauté française et la Région wallonne ont fait de même[358].

82.- Une compétence limitée. Si les collectivités fédérées sont habilitées à décider, dans l'exercice de leurs compétences, des cas et des conditions dans lesquels une atteinte à la vie privée des citoyens est permise, cela ne signifie pas pour autant qu'elles peuvent agir tout à fait librement. En effet, la Cour constitutionnelle et la section de législation du Conseil d'État[359] soutiennent que les décrets et les ordonnances doivent respecter la loi du 8 décembre 1992.

La loi fédérale est, selon la Cour constitutionnelle, « la réglementation fédérale générale, qui a valeur de réglementation minimale pour toute

---

et le fédéralisme », *in Les droits fondamentaux en Belgique* (dir. M. Verdussen et N. Bonbled), *op. cit.,* pp. 248 à 251 et 259 à 261 ; M. Melchior et C. Courtoy, « La limitation des droits fondamentaux », *in Les droits fondamentaux en Belgique* (dir. M. Verdussen et N. Bonbled), *op. cit.,* pp. 277 à 281.

[356] C.C., arrêt n° 50/2003, du 30 avril 2003, p. 23, B.8.10. Voy. également, C.C., arrêt n° 51/2003, du 30 avril 2003, B.4.12 ; avis L. 37.288/3, *op. cit.*, p. 162 ; J.-M. Hausman, « Le droit d'accès au système d'information santé organisé par le décret du 16 juin 2006 de la Communauté flamande », *in Évolution des droits du patient, indemnisation sans faute des dommages liés aux soins de santé : le droit médical en mouvement* (dir. G. Schamps), Bruxelles, Bruylant, Paris, L.G.D.J., 2007, p. 205, n° 18 ; J. Velaers, « De samenloop van grondrechten in het Belgische rechtsbestel », *in Samenloop van grondrechten in verschillende rechtsstelsels* (dir. A. Nieuwenhuis, L. Dragstra, J. Velaers, L. Huybrechts, H. Wolswijk, F. Salomons, B. de Groot et S. Voet), Den Haag, Boom Juridische uitgevers, 2008, pp. 154 et 155, n° 5 ; M. Verdussen et A. Noël, « Les droits fondamentaux et la réforme constitutionnelle de 1993 », *A.P.T.,* 1994, p. 130 ; S. Van Drooghenbroeck et J. Velaers, « La répartition des compétences dans la lutte contre la discrimination », *in De nieuwe federale antidiscriminatiewetten – Les nouvelles lois luttant contre la discrimination* (dir. C. Bayart, S. Sottiaux et S. Van Drooghenbroeck), die Keure, La Charte, Brugge, Bruxelles, 2008, pp. 106 et 107.

[357] Décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, *M.B.,* 29 octobre 2008.

[358] Accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.*, 23 juillet 2013. Voy. *infra*, n°s 233.- et s.

[359] Le rôle de la section de législation du Conseil d'État et de la Cour constitutionnelle est détaillé dans la Titre III de la présente recherche. Voy. infra n^{os}421.- et s. et n°s 434.- et s.

la matière »[360]. Pour la section de législation du Conseil d'État, la loi du 8 décembre 1992 est « la loi de base »[361] en la matière à laquelle une autre norme de valeur législative ne pourrait déroger en diminuant la protection prévue par le législateur fédéral[362].

> Par exemple, à propos du décret flamand relatif au système d'information concernant la santé, la section de législation du Conseil d'État a affirmé que le législateur décrétal était compétent pour compléter la loi du 8 décembre 1992 mais qu'il ne pouvait y déroger[363].

II. Une solution insatisfaisante

83.- Une solution de compromis. La soumission des décrets et des ordonnances à la loi du 8 décembre 1992 réalise un compromis louable entre deux impératifs.

D'une part, confier la réglementation minimale de la matière au législateur fédéral respecte la volonté originaire du Constituant[364] et du législateur[365] d'harmoniser, sur le territoire de la Belgique, la protection de la vie privée, notamment dans le cadre des traitements de données à caractère

[360] C. C., arrêt n° 162/2004 du 20 octobre 2004, B.5.2. ; C. C., arrêt n° 16/2005 du 19 janvier 2005, B.5.2. ; C. C., arrêt n° 15/2008, du 14 février 2008, B. 21 ; J.-M. HAUSMAN, « Le droit d'accès au système d'information santé organisé par le décret du 16 juin 2006 de la Communauté française », *in Évolution des droits du patient, indemnisation sans faute des dommages liés aux soins de santé : le droit médical en mouvement* (dir. G. SCHAMPS), Bruxelles, Bruylant, Paris, L.G.D.J., 2007, pp. 187-247 et spéc. pp. 204-207.

[361] Avis L. 37.288/3, *op. cit.,* p. 163, note 7 ; avis L. 33.285/1 du 2 mai 2002, sur un avant-projet de loi portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce et création des guichets d'entreprise, *Doc. Parl.,* Chambre, session 2002-2003, n° 50 2058/001, p. 105 ; avis du 19 juillet 1994 relatif à un projet d'arrêté royal organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale, *M.B.,* 3 avril 1997.

[362] Avis L. 37.288/, *op. cit.,* p. 163 ; avis L. 33.285/1, *op. cit.,* p. 105.

[363] Avis L. 37.288/3 des 6, 12 et 15 juillet 2004, à propos d'un avant-projet de décret « betreffende het gezondheidsinformatiesysteem », *Parl. St.,* Vl. Parl., 2005-2006, n° 531/1, p. 163.

[364] Rapport fait au nom de la Commission de révision de la Constitution, des réformes institutionnelles et du règlement des conflits relatif à la Révision du titre II de la Constitution en vue d'y insérer un article 24*quater* relatif au respect de la vie privée, *Doc. Parl.,* Ch. Repr., session 1993-1994, n° 1278/2, p. 3.

[365] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel et proposition de loi relative à la protection de données personnelles concernant les personnes physiques dans les fichiers informatiques ou banques de données et à la création d'une commission nationale de l'informatique et des libertés, Rapport fait au nom de la Commission de la Justice par Mme Merckx-van Goey, *Doc. Parl.,* Chambre, session 1991-1992, n° 413/12, p. 15.

personnel. En effet, au moment de l'adoption de la loi du 8 décembre 1992 et de l'insertion de l'article 22 dans la Constitution, prévalait l'idée que l'aménagement des droits fondamentaux relevait de la compétence exclusive du législateur fédéral. Il était avancé que de tels attributs de la personne humaine devaient être interprétés et mis en œuvre de manière uniforme sur tout le territoire. La loi du 8 décembre 1992 a donc été adoptée dans le but d'« instaurer une réglementation générale qui constitue une exigence minimale pour les législations sectorielles »[366]. Dans le même sens, à l'occasion de l'adoption de l'article 22 de la Constitution, le constituant a affirmé notamment que « les restrictions du droit au respect de la vie privée relèvent exclusivement des compétences fédérales »[367].

D'autre part, permettre aux communautés et aux régions d'intervenir en la matière reflète l'évolution du fédéralisme belge. Les communautés et les régions exercent aujourd'hui de nombreuses compétences ayant un impact sur les droits fondamentaux et notamment sur la protection de la vie privée. Il serait artificiel de continuer à soutenir que ces entités ne sont pas compétentes pour poser des limites à l'exercice de ces droits[368].

84.- Une solution critiquable. Bien qu'elle soit modérée, cette solution surprend. Elle aboutit à soumettre les décrets et les ordonnances au respect d'une autre norme de valeur législative et à ébrécher ainsi les principes qui sous-tendent l'organisation fédérale de l'État belge[369]. En effet, contraindre les législateurs communautaires et régionaux à respec-

---

[366] *Idem.*

[367] Rapport fait au nom de la Commission de révision de la Constitution, des réformes institutionnelles et du règlement des conflits relatif à la Révision du titre II de la Constitution en vue d'y insérer un article 24*quater* relatif au respect de la vie privée, *op. cit.*, p. 3.

[368] X. Delgrange et B. Lombaert, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : questions d'actualité », *in La motivation formelle des actes administratifs* (dir. P. Jadoul et S. Van Drooghenbroeck), Bruxelles, La Charte, 2005, pp. 8-11. Selon la section de législation du Conseil d'État, une telle interprétation était devenue absurde (avis L. 37.288/3, des 6, 12 et 15 juillet 2004, à propos d'un avant-projet de décret « betreffende het gezondheidsinformatiesysteem », *Parl. St.,* Vl. Parl., 2005-2006, n° 531/1, p. 162.

[369] Cette solution s'apparente d'ailleurs davantage au modèle du fédéralisme d'exécution qui prévaut en Allemagne ou en Suisse, qu'au modèle fédéral belge En effet, la Loi fondamentale allemande confie aux *Länders* une compétence générale d'exécution des lois, sous la surveillance du *Bund* qui dispose de divers procédés de tutelle à leur égard. En Suisse, les cantons ne disposent pas d'une telle habilitation constitutionnelle mais ils se voient fréquemment confier l'exécution de lois fédérales. À ce sujet, voy. R. Ergec, « Les aspects juridiques du fédéralisme », *Le fédéralisme. Approches politique, économique et juridique,* Bruxelles, De Boeck Université, 1994, p. 68 ; H. Bribosia et J.-L. Van Boxstael, *Le partage des compétences dans la Belgique fédérale,* Brugge, La Charte, 1994, pp. 78-83 ; M. Verdussen, « Évolution du fédéralisme, de la décentralisation et du régionalisme », *Cinquante ans de constitutionnalisme. Réalité et perspectives (1945-1995),* Bâle, Genève, Munich, Helbing & Lichtenhahn,

ter le prescrit du législateur fédéral méconnaît le principe de l'exclusivité des compétences de chaque collectivité, applicable dans notre système fédéral. Selon ce principe, la collectivité fédérale et les collectivités fédérées interviennent seules, à l'exclusion l'une de l'autre, dans les matières qui leur appartiennent. Elles sont placées sur un pied d'égalité, et ne peuvent être subordonnées l'une à l'autre.

Cette égalité entre les composantes de l'État fédéral concerne au premier chef les normes adoptées par les législateurs communautaires et régionaux, comme l'affirme l'article 19, § 2, de la loi spéciale du 8 août 1980 qui consacre l'équipollence entre les lois et les décrets. Ces normes ne sont donc soumises qu'au respect de la Constitution et des lois spéciales et ordinaires qui organisent le partage des compétences entre ces collectivités[370].

85.- Le recours à la loi spéciale. Pour l'heure, la compétence du législateur fédéral d'édicter des normes générales, qui s'imposent aux communautés et aux régions, ne jouit donc d'aucun fondement juridique.

Une solution à cette lacune serait de recourir à la loi spéciale du 8 août 1980 et d'y intégrer une disposition suivant laquelle, dans l'exercice de leurs compétences, les communautés et les régions doivent respecter les règles fédérales générales en matière de protection des données à caractère personnel. Outre que cette solution offrirait un fondement juridique à la compétence complémentaire des communautés et des régions, elle respecterait davantage la hiérarchie des normes en évitant qu'il faille, par une interprétation jurisprudentielle, faire prévaloir une norme de valeur législative par rapport à d'autres normes de même valeur.

C'est, du reste, la solution qui prévaut en matière de marchés publics, par exemple. L'article 6, § 1, VI, alinéa 4, de la loi spéciale du 8 août 1980 confie au législateur fédéral le soin de définir les règles générales en

---

1999, pp. 244-245 ; F. Delpérée, *Le droit constitutionnel de la Belgique,* Bruxelles, Paris, Bruylant, L.G.D.J., 2000, pp. 597, 588 et 589 ; F. Delpérée et M. Verdussen, « L'égalité, mesure du fédéralisme », *R.B.D.C.,* 2004, pp. 295-298.

[370] R. Ergec, « Les aspects juridiques du fédéralisme », *op. cit.,* pp. 43 à 45 ; H. Bribosia et J.-L. Van Boxstael, *op. cit.,* pp. 39-40 ; B. Jadot, « La jurisprudence de la Cour d'Arbitrage et le système constituionnel », *in La Cour d'Arbitrage. Actualités et perspectives,* Bruxelles, Bruylant, 1998, pp. 230-232 ; M. Verdussen, « Évolution du fédéralisme, de la décentralisation et du régionalisme », *op. cit.*, pp. 228, 230, 231, 238 et 239 ; M. Uyttendaele, *Précis de droit constitutionnel belge, op. cit.*, p. 918 ; F. Délpérée, *Le droit constitutionnel de la Belgique, op. cit.*, p. 588 ; A. Alen, *Handboek van het Belgisch Staatsrecht,* Deurne, Kluwer, 1995, p. 340 ; L.P. Suetens et R. Leysen, « Staat, gewesten en gemeenschappen. De technieken van bevoegdsverdeling. De rol van het arbitragehof », *in Prof. Dr Louis Paul Baron Suetens, Op de grens van het ideaal denkbare en het praktisch haalbare,* Brugge, die Keure, 1997, pp. 224 et 225 ; F. Delpérée et M. Verdussen, *op. cit.*, pp. 291-294.

matière de marchés publics, tandis que les régions sont compétentes pour compléter cette réglementation de base, sans toutefois pouvoir y déroger. Cette solution vise à garantir le maintien de l'union économique et monétaire sur le territoire belge[371].

Néanmoins, cette solution laisse subsister des difficultés. Comment déterminer les aspects de la matière qui forment les « règles générales » ? La Cour constitutionnelle serait sans doute amenée à devoir éclairer cette notion, comme elle l'a fait en matière de marchés publics à propos de l'organisation de l'agréation des entrepreneurs[372]. Plus particulièrement, les règles générales consisteraient-elles exclusivement en les principes fondamentaux qui sous-tendent la protection des données à caractère personnel, ou s'agirait-il également de la procédure applicable lors des traitements de ces données ?

> Par exemple, actuellement, la loi du 8 décembre 1992 institue la Commission de la protection de la vie privée, auprès de la Chambre des représentants[373]. Cette autorité chargée de la protection des données est composée de membres désignés par la Chambre des représentants, chargés notamment d'émettre des avis à propos de « l'application des principes fondamentaux de la protection de la vie privée »[374], que ceux-ci concernent des traitements de données effectués au sein de l'administration fédérale ou des administrations fédérées. L'intervention de cette Commission fait partie de la procédure encadrant les traitements de donnés à caractère personnel. Doit-on considérer qu'il s'agit d'une règle générale applicable aux entités fédérées[375] ?

Une autre question se poserait également dans l'hypothèse où le législateur fédéral n'aurait pas (encore) réglé une question qui semblerait relever de la législation de base. Les législateurs communautaires et régionaux devraient-ils attendre son intervention avant de pouvoir réglementer certains aspects de la question ? Si l'on s'en réfère à la matière des marchés publics, il semble admis que les communautés et les régions ne doivent pas attendre la réglementation fédérale pour intervenir. Mais, si les autorités fédérées interviennent, les normes adoptées seront soumises aux

---

[371] Exposé des motifs du projet de loi modifiant la loi spéciale du 8 août 1980 de réformes institutionnelles, *Doc. Parl.,* Chambre, S.E. 1988, n° 516/1, p. 10 ; B. HAUBERT et P. VANDERNOOT, « La nouvelle loi de réformes institutionnelles », *A.P.T.,* 1988, p. 241 ; A. ALEN, *op. cit.,* p. 342 ; C.C., arrêt n° 32/92, du 23 avril 1992, p. 16, B.3.2.

[372] C.C., arrêt n° 79/92, du 23 décembre 1992.

[373] Voy. les art. 23 à 36 de la loi du 8 décembre 1992. Sur le statut de cette Commission, voy. E. DEGRAVE, « La Commission de la protection de la vie privée : un organisme invincible ? », *R.D.T.I.,* 2006, pp. 225 à 241.

[374] Art. 29, § 1, de la loi du 8 décembre 1992.

[375] À ce sujet, voy. D. DE ROY, C. DE TERWANGNE et Y. POULLET, « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », *C.D.P.K.,* 2007, p. 332.

modifications ultérieures de la législation fédérale. La compétence que les législateurs communautaires et régionaux auraient exercée jusqu'alors serait ainsi limitée[376].

Le troisième chapitre proposera des solutions pour résoudre ces difficultés[377].

Section 2. L'e-gouvernement et la compétence du législateur

86.- Une matière réservée au législateur. En Belgique, toute ingérence dans le droit à la protection de la vie privée doit être organisée par le législateur. Le mot « loi » prévu à l'article 22 de la Constitution s'entend en effet d'une loi au sens formel du terme. L'article 22 de la Constitution diffère à cet égard de l'article 8 de la Convention européenne des droits de l'homme, qui ne requiert qu'une loi au sens matériel du terme[378].

La Cour constitutionnelle l'a déjà rappelé à plusieurs reprises, affirmant que « bien que, en utilisant le mot 'loi', l'article 8.2 de la Convention européenne [des droits de l'homme] n'exige pas que l'ingérence qu'il permet soit prévue par une 'loi', au sens formel du terme, le même mot 'loi' utilisé à l'article 22 de la Constitution désigne une disposition législative »[379].

L'e-gouvernement compromet le respect de cette exigence de légalité, ce qui contribue au « déclin de l'État de droit »[380] qui se manifeste depuis plusieurs années dans maints domaines du droit, mais apparaît clairement dans l'e-gouvernement. On en dresse le constat au travers de plusieurs exemples.

Partant de là, il convient ensuite de s'interroger sur le contenu à donner aujourd'hui aux lois qui encadrent l'e-gouvernement, en veillant

---

[376] H. Bribosia et J.-L. Van Boxstael, *op. cit.,* p. 76 et p. 87.

[377] Voy. en particulier *infra,* n°s 227.- et s.

[378] J. Vande Lanotte et G. Goedertier, *Handboek Belgisch Publiekrecht*, Brugge, die Keure, 2010, pp. 448- 449, n° 688 ; P. De Hert, « Artikel 8. Recht op privacy »*, in Handboek EVRM, Deel 2. Artikelsgewijze commentaar* (dir. J. Vande Lanotte et Y. Haeck), Anvers, Intersentia, 2004, pp. 716-718 ; M. Melchior et C. Courtoy, *op. cit.,* p. 284 ; R. Andersen et C. Behrendt, « La protection des droits constitutionnels »*, in Les droits fondamentaux en Belgique* (dir. M. Verdussen et N. Bonbled), *op. cit.,* p. 356.

[379] C.C., arrêt n° 151/2006, du 18 octobre 2006, B. 5.6. Voy. égal. C.C., arrêt n° 29/2010, du 18 mars 2010, p. 19, B. 10.2. ; C.C., arrêt n° 202/2004 du 21 décembre 2004, B.4.3.

[380] P. Quertainmont, « Le déclin de l'État de droit », *J.T.,* 1984, pp. 273 et s.

à respecter tant que faire ce peut l'exigence de légalité tout en tenant compte des mutations engendrées par l'usage des technologies au sein de l'administration.

I. La raison d'être de l'exigence de légalité confrontée à l'e-gouvernement

87.- Deux justifications. Deux justifications expliquent l'exigence de légalité requise par l'article 22 de la Constitution. L'intervention du législateur doit garantir qu'un débat démocratique soit mené dès qu'il est porté atteinte à la vie privée des individus, et que la norme organisant une telle ingérence soit accessible et prévisible.

L'e-gouvernement ébranle ces impératifs.

A. La raison d'être de la loi

88.- Le débat démocratique. En imposant une loi au sens formel du terme pour encadrer chaque ingérence dans la protection de la vie privée des citoyens, l'article 22 de la Constitution entend garantir que l'instauration d'un traitement de données à caractère personnel soit soumise à un débat démocratique.

La Cour constitutionnelle et la section de législation du Conseil d'État ont plusieurs fois souligné que le débat démocratique est une garantie pour la protection de la vie privée des citoyens. Ainsi affirment-elles qu'« en plaçant la protection de la vie privée sous la sauvegarde de la loi elle-même, le constituant a entendu que les cas et les conditions dans lesquels il pourrait y être porté atteinte soient soumis à la décision d'assemblées délibérantes démocratiquement élues »[381]. L'intervention des parlementaires doit être assurée car « c'est précisément là où les risques pour la protection de la vie privée sont les plus grands, que le législateur

[381] Avis L. 37.765/1/2/3/4 du 4 novembre 2004 sur un avant-projet de loi-programme, *Doc. Parl.*, Chambre, 2004-2005, n° 1437 ; avis L. 37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc. Parl.*, Chambre, 2004-2005, n° 1598/1 et 1599/1, cités par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2004 », *R.B.D.C.*, 2005/2, p. 260, n° 6 ; C.C., arrêt n° 202/2004, du 21 décembre 2004, B.4.3. et B.6.3. ; C.C., arrêt n° 95/2008, du 26 juin 2008, B.42 ; C.C., arrêt n° 29/2010, du 18 mars 2010, B. 16.1 ; C.C., arrêt n° 6/2013, du 14 février 2013, B.5.7 ; C.C., arrêt n° 66/2013, du 16 mai 2013, B.11.1.

doit être associé de la manière la plus directe qui soit à la confection des normes »[382].

En d'autres termes, c'est l'idée qu'il est plus prudent de conférer aux élus de la Nation le soin de déterminer les limitations portées aux droits fondamentaux, plutôt que de « recourir aux responsables de l'ordre public, soit au gouvernement et aux autorités locales, [ce qui établirait] une confusion entre celui qui fait la règle et celui qui est tenu de la respecter »[383]. Comme il en sera question plus loin[384], dans l'e-gouvernement, chaque traitement de données à caractère personnel doit incarner un juste équilibre entre l'efficacité de l'administration et la protection de la vie privée des citoyens.

L'exigence de légalité impose de confier cette tâche au législateur et non à l'administration elle-même. Si l'organisation de traitements de données était laissée à la discrétion des administrations, celles-ci pourraient avoir tendance à apprécier la nécessité de tels traitements principalement au regard de leur intérêt immédiat, celui de l'efficacité administrative, et de donner trop peu de poids à la protection de la vie privée des citoyens.

Pour le dire autrement, si cette tâche n'était pas assumée par le pouvoir législatif, cela reviendrait « pour le législateur, désigné par la Constitution comme le gardien du respect du droit au respect de la vie privée, [à renoncer] à définir lui-même quelles sont les intrusions qui peuvent venir restreindre le droit dont il a la garde. L'article 22 de la Constitution lui interdit de faire ce choix »[385].

89.- L'accessibilité et la prévisibilité de l'ingérence. L'article 22 de la Constitution impose non seulement au législateur d'intervenir, mais il doit encore le faire de manière particulièrement rigoureuse, afin que la loi soit accessible et compréhensible[386]. Cette exigence est reprise dans la jurisprudence de la Cour constitutionnelle.

---

[382] Avis L. 33.487/1/3 des 18 et 20 juin 2002 sur un avant-projet de loi « portant des mesures en matière de soins de santé », *Doc. Parl.*, Chambre, sess. 2002-2003, n° 2125/1, p. 539.

[383] F. Delpérée, *Le droit constitutionnel de la Belgique*, *op. cit.*, p. 193, n° 180.

[384] Voy. *infra,* n°s 136.- et s.

[385] SLCE, avis du 2 février 1998 relatif à un avant-projet de loi « transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *Doc. Parl.*, Ch. Repr., session 1997-1998, n° 49 1566/1, p. 201.

[386] J.-P. Queneudec, « Liberté d'accès au droit et qualité des règles juridiques », *Libertés, justice, tolérance – Mélanges en hommage au doyen Gérard Cohen-Jonathan,* vol. II, Bruxelles,

> La Cour constitutionnelle rappelle ainsi que l'article 22 de la Constitution « garantit à tout citoyen qu'il ne pourra être porté atteinte au respect de sa vie privée qu'en vertu d'une disposition législative, et dans les conditions que celle-ci prévoit, de manière à ce que chacun puisse savoir à tout moment à quelles conditions et dans quelles circonstances les autorités publiques pourraient s'ingérer dans ce droit »[387].

Ainsi, la loi doit être *accessible,* ce qui signifie que toute personne « doit pouvoir disposer de renseignements suffisants [...] sur les normes juridiques applicables à un cas donné »[388].

> Dans une affaire récente soumise à la Cour européenne des droits de l'homme[389], il est question d'une base de données de surveillances secrètes, constituée par le Département intérieur des transports russes et contenant le nom des personnes considérées comme des extrémistes potentiels, tels que les *skinheads* et les militants des droits de l'homme. Chaque fois qu'une de ces personnes achète un ticket de train ou d'avion, le Département intérieur des transports en est immédiatement informé. Un militant des droits de l'homme, Sergey Shimovolos, est enregistré dans cette base de données. En prenant le train pour rejoindre le Sommet de l'Union européenne-Russie en 2007, il est arrêté par la police, qui contrôle son identité et le contraint de le suivre au poste de police où il subit un interrogatoire sur l'objet de son voyage, notamment. La Cour européenne des droits de l'homme considère qu'en enregistrant les données de Monsieur Shimovolos, les autorités russes violent l'article 8 de la Convention européenne des droits de l'homme car la base de données est organisée par un arrêté ministériel qui n'a pas été publié ni rendu accessible au public[390].

En outre, ces normes doivent être suffisamment *compréhensibles et prévisibles*. Une telle clarté doit permettre à tout individu de connaître les conséquences que la loi réserve à ses actes.

> Comme l'affirme la Cour européenne des droits de l'homme, la loi doit être « énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant, au besoin, de conseils éclairés, il doit être à même

---

Bruylant, 2004, p. 1317 ; Voy. not. Cour eur. D.H., arrêt *Malone c. Royaume-Uni*, 2 août 1984, req. n° 8691/79, § 67. Ces garanties ont été appliquées aux traitements de données dans l'arrêt *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95, §§ 52 et 55.

[387] C.C., arrêt n° 202/2004, du 21 décembre 2004, B.4.3. Voy. égal. C.C., arrêt n° 66/2013 précité, B.11.1.

[388] Voy. not. Cour eur. D.H., arrêt *Sunday Times c. Royaume-Uni*, 26 avril 1979, req. n° 6538/74, § 49.

[389] Cour eur. D.H., arrêt *Shimovolos v. Russia,* 21 juin 2011, req. 30194/09.

[390] *Ibid.,* §§ 69 et 70.

de prévoir, à un degré raisonnable, les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé »[391].

Montesquieu, déjà, s'interrogeant sur ce qu'est une « bonne loi », avançait les caractéristiques suivantes :

« – le style doit être simple et concis, la loi ne doit pas contenir d'expressions vagues, elle ne doit pas être subtile car elle est faite pour des gens de médiocre entendement ;

– il faut éviter les exceptions et les limitations car de pareils détails jettent dans de nouveaux détails ; comme les lois inutiles affaiblissent les lois nécessaires, celles qu'on peut éluder affaiblissent la législation [...] ;

– enfin, il ne faut point de changement de loi sans une raison suffisante »[392].

La précision de la loi s'explique également par le souci d'encadrer l'action du pouvoir exécutif et de contrôler les abus de pouvoir. C'est pourquoi, toute personne doit connaître « l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré »[393].

La lisibilité des textes organisant des ingérences dans la vie privée importe particulièrement lorsqu'il est question de traitements de données à caractère personnel. En effet, l'utilisation d'informations personnelles fait peur aux citoyens car les outils nouveaux de traitements de données paraissent complexes et opaques. Les personnes concernées craignent également que l'objectif poursuivi lors de la collecte de leurs informations ne soit détourné et se retourne finalement contre eux. L'exigence de prévisibilité de la norme prend dès lors tout son sens pour établir la confiance entre les citoyens et l'État qui met en place de tels outils.

Remarquons, enfin, que l'article 22 de la Constitution impose ainsi au législateur un travail plus rigoureux que l'article 105 de la Constitution évoqué dans les premières lignes de ce chapitre. En effet, puisque le législateur doit veiller à ce que les citoyens connaissent et comprennent les atteintes portées à leur vie privée, il ne peut se contenter d'intervenir. Il doit rédiger une loi ayant un contenu assez précis, que l'on détaille plus loin[394]. On constate ainsi que la protection de la vie privée ajoute à la

[391] Voy. not. Cour eur. D.H., arrêt *Sunday Times c. Royaume-Uni*, du 26 avril 1979, req. n° 6538/74 ; arrêt *Malone c. Royaume-Uni*, du 2 août 1984, § 67 ; arrêt *Amann c. Suisse*, du 16 février 2000, req. n° 27798/95, §§ 75 et 76 et arrêt *Leander c. Suède*, du 26 mars 1987, req. n° 9248/81, § 50.

[392] MONTESQUIEU, *De l'esprit des lois,* Paris, Garnier, 1927, Livre 29, Chapitre XVI.

[393] Voy. not. Cour. eur. D.H., arrêt *Amann c. Suisse*, 16 février 2000, req. n° 27798/95, § 62.

[394] Voy. *infra,* n°s 99.- et s.

légalité formelle le respect d'exigences relatives à la légalité substantielle de la loi qui organise un traitement de données à caractère personnel[395].

B. La raison d'être de la loi ébranlée par l'e-gouvernement

90.- Le déclin de la loi. La loi est malade et se dévalorise. Jadis respectée en tant qu'expression de la volonté générale, elle a aujourd'hui « perdu son lustre et sa majesté [...] parce qu'elle est devenue une règle de droit parmi d'autres, soumise à des contrôles, concurrencée par des règles fondées sur d'autres légitimités »[396]. La qualité de la loi s'en ressent. « Les lois sont nombreuses et instables, souvent mal rédigées, elles portent fréquemment sur des points de détail et sont parfois dépourvues d'effectivité. L'altération profonde des qualités de la loi contamine l'ensemble du système juridique et menace tant le respect des lois, que la sécurité juridique des citoyens »[397].

Le déclin de la loi s'étend, de manière générale, à toutes les matières qui sont encadrées par le législateur[398]. Néanmoins, ce phénomène se manifeste de manière particulièrement nette dans l'e-gouvernement, comme l'illustrent les développements qui suivent.

Doit-on s'en inquiéter ? En amenuisant le rôle du législateur, l'e-gouvernement laisse de plus en plus de place au pouvoir exécutif. On ne peut s'y opposer totalement, dans la mesure où certaines questions d'e-gouvernement gagnent à être réglées par le pouvoir exécutif plutôt que le législateur. On pense, en particulier, aux aspects techniques d'un

[395] Pour une illustration de ce constat à propos des concessions de service public, voy. E. Degrave et Y. Poullet, « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée », *J.T.,* 2008., pp. 279 et 280.

[396] B. Mathieu, *La Loi,* Paris, Dalloz, 1996, p. 73.

[397] *Ibid.,* p. 77.

[398] D'une manière générale, l'inflation législative, comme en matière de sécurité sociale, par exemple, aboutit à un foisonnement de normes éparses et de concepts flous rendant le corpus normatif très complexe. L'adoption, dans divers domaines, de lois-programmes, de lois « portant des dispositions diverses », notamment, laissent deviner un amaigrissement du débat démocratique. Par ailleurs, la multiplication d'organismes décentralisés, ayant des statuts peu homogènes, dont certains ont une large autonomie et sont soumis à un contrôle allégé (comme les entreprises publiques autonomes), montre l'érosion du pouvoir du législateur d'encadrer l'action administrative (à ce sujet, voy. P. Jadoul, B. Lombaert et F. Tulkens (dir.), *Le paraétatisme. Nouveaux regards sur la décentralisation fonctionnelle en Belgique et dans les institutions européennes,* Bruxelles, La Charte, 2010).

nouvel outil de traitement de données qui peuvent difficilement faire l'objet d'un réel débat d'idées au Parlement[399].

Il n'en demeure pas moins que l'utilisation des données à caractère personnel touche au droit fondamental à la vie privée. Le respect effectif de cette valeur dans notre État démocratique mérite donc que les représentants du peuple débattent de certains aspects des traitements de données, afin d'endiguer les menaces qui planent dans l'e-gouvernement, et qu'ils s'attèlent ensuite à ancrer leurs décisions dans des normes accessibles et claires. On pense, notamment, à la proportionnalité d'un outil de traitement de données. Faut-il mettre en place une base de données centralisant de multiples informations personnelles, ou est-il préférable de recourir à une plateforme d'échanges d'informations ? L'utilisation d'un identifiant unique dans tel réseau sectoriel n'est-elle pas dangereuse ? La finalité d'un outil est également un élément de débat important, conduisant le législateur à réfléchir à la légitimité de son action[400].

§1. L'appauvrissement du débat démocratique

91.- Considérations générales. Le législateur est-il dépassé par la complexité des questions liées à l'usage des technologies, et l'ampleur de la tâche que représente la protection des données à caractère personnel en ce domaine ? On constate en tout cas que des aspects substantiels de l'e-gouvernement sont organisés par une loi peu claire, voire aucune loi.

92.- L'absence de loi. Certains traitements de données ne sont pas organisés par une loi. Ils n'ont donc pas été discutés par les élus du peuple.

> C'est le cas, par exemple, de l'entrepôt de données OASIS décrit précédemment[401]. Rappelons que cet outil de profilage très puissant regroupe un grand nombre de données à caractère personnel provenant de sources authentiques diverses. Ces données sont ensuite soumises à des calculs mathématiques permettant d'identifier avec un haut degré de certitude, les personnes ayant commis une fraude sociale. Bien qu'OASIS augmente considérablement la puissance de l'administration qui l'utilise, cet outil n'a pas été créé par une loi, ni même un arrêté royal. Seules trois décisions de comité sectoriel l'encadrent.

---

[399] Ainsi en va-t-il, par exemple, de l'ordre dans lequel apparaissent les chiffres qui composent le numéro d'identification du registre national. À juste titre selon nous, celui-ci est déterminé par l'arrêté royal du 3 avril 1984 relatif à la composition du numéro d'identification des personnes isncrites au Registre national des personnes physiques, *M.B.,* 21 avril 1984.

[400] Voy. *infra,* n°s 112.- et s.

[401] Voy. *supra,* n°s 44.- et s.

93.- Des lois « fourre-tout ». Des traitements de données sont, certes, prévus par une loi, mais il s'agit d'une « loi-programme » ou d'une « loi portant des dispositions diverses », qui sont des lois « fourre-tout ». Noyés parmi une multitude de dispositions à adopter, on peut raisonnablement douter de la qualité des débats parlementaires consacrés aux outils qu'elles prétendent encadrer. Bien souvent d'ailleurs, la lecture des travaux préparatoires confirme de telles craintes. Il arrive ainsi que par cette voie soient adoptées des règles « qui n'auraient pu aisément franchir le cap de délibérations législatives traditionnelles »[402].

> Par exemple, récemment a été créée la Banque-Carrefour des permis de conduire. Il s'agit, en réalité, d'une source authentique de données qui centralise 12 informations relatives au permis de conduire et à son titulaire (numéro d'identification au Registre national, numéro de permis de conduire, mentions additionnelles ou restrictives, etc.). Grâce à cette base de données, chaque citoyen disposera prochainement d'un permis de conduire sous forme de carte bancaire qui permettra notamment aux « acteurs de la police et de la justice [d'avoir] toujours immédiatement accès à toutes les informations disponibles concernant un conducteur et pourront, dès lors, prendre les mesures les plus adaptées »[403] lors des contrôles. La presse a dénoncé le fait que, concrètement, grâce à cette banque de données, les juges auront connaissance de tous les procès-verbaux et règlements transactionnels pour excès de vitesse des personnes comparaissant devant eux et pourront dès lors tenir compte, dans leur décision, de leur antécédent, ce qui n'était pas possible jusqu'alors puisque seules les condamnations judiciaires figurent dans le casier judiciaire[404]. Bien que cela aurait mérité un débat de fond sur les tenants et aboutissants de cet enregistrement de données, la Banque-Carrefour des permis de conduire a été créée par une loi « portant des dispositions diverses » contenant 94 dispositions. Il est également piquant de constater que le gouvernement ayant déposé le projet était en affaires courantes. On ne peut que regretter le caractère expéditif des réflexions menées, dont témoignent les maigres discussions préparatoires[405].

---

[402] P. Quertainmont, *op. cit.,* p. 275.

[403] Rapport fait au nom de la Commission de l'infrastructure, des communications et des entreprises publiques par Mme K. Temmerman relatif au projet de loi portant des dispositions diverses (art. 4 à 25), *Doc. Parl.,* Ch. Repr., sess. 2010-2011, n° 53-1208/11, p. 7.

[404] http://www.rtbf.be/info/societe/detail_tous-les-pv-repris-sur-le-permis-de-conduire-press ?id=6091233 (article du 12 mai 2011).

[405] Pour un autre exemple frappant, voy. la loi du 1er mars 2007 portant des dispositions diverses (III) (*M.B*, 14 mars 2007) qui comprend 165 dispositions. 39 d'entre elles modifient la loi sur la Banque-Carrefour de la sécurité sociale, auxquelles les discussions préparatoires n'ont consacré que quelques brèves explications (voy. le Rapport fait au nom de la Commission des affaires sociales par Mme Maggie De Block concernant le projet de loi portant des dispositions diverses (III) [art. 34 à 61, art. 68 à 80 et art. 87 à 89], *Doc. Parl.,* Ch. Repr., sess. 2006-2007, n° 51- 2788/013, 24 janvier 2007, pp. 11-15).

> Remarquons qu'il y a quelques années, un avant-projet de loi-programme insérait la mention de la « filiation » dans le Registre national. La section de législation du Conseil s'est prononcée défavorablement en affirmant qu' « un texte qui modifie la substance du Registre national [...] n'a pas sa place dans une loi-programme »[406]. Cette mention n'a finalement pas été intégrée.

94.- Des initiatives gouvernementales. La plupart des lois qui encadrent l'e-gouvernement ont été adoptées à l'initiative du gouvernement[407]. Concrètement, on peut craindre que le pouvoir de faire la loi appartienne ainsi davantage au Gouvernement qu'au Parlement. Etant donné que la coalition gouvernementale est soutenue par une majorité parlementaire, les propositions de loi émanant de l'opposition, ou les amendements parlementaires qui modifient le projet de loi initial, risquent souvent de ne pas aboutir[408].

95.- La transposition d'une directive. L'organisation des traitements de données à caractère personnel est soumise au respect d'une directive européenne, la directive 95/46. Or, on constate que « l'idée de souveraineté parlementaire [...] est fortement ébranlée par le droit communautaire et l'exercice de la fonction législative, subordonnée, d'application du droit communautaire »[409]. Bien souvent, les règles européennes sont des règles techniques, que les législateurs nationaux peuvent être tentés de

---

[406] SLCE, avis n° 37.765/1/2/3/4, *op. cit.,* p. 633.

[407] Tel est le cas notamment du Registre national (voy. le projet de loi du 28 juin 1982 organisant un registre national des personnes physiques, *Doc. Parl.,* Ch. Repr., session 1982-1983, n° 296/1 ; le projet de loi du 15 janvier 2003 modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *Doc. Parl.,* Ch. Repr., session 2002-2003, n° 50-2226/001) ainsi que de la Banque-Carrefour de la sécurité sociale (voy. Projet de loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *Doc. Parl.,* Ch. Repr., session 1988-1989, n° 899/1, repris dans *Pasin.,* 1990, I, pp. 76 et s.

[408] P. Quertainmont, *op. cit.,* p. 277 ; B. Mathieu, *La loi, op. cit.,* pp. 88 et s. Pour un exemple relatif aux règles de traitements des données à caractère personnel voy. le rejet de l'amendement proposé par un parlementaire au sujet des critères de réutilisation des données (Projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *Doc. Parl.,* Ch. Repr., sess. 1997-1998, n n° 1566/10, p. 90).

[409] B. Mathieu, *La loi, op. cit.*, p. 48. Dans le même sens, X. Bioy et P. Raimbault, « La puissance de la Loi en question », *in La puissance publique à l'heure européenne* (dir. P. Raimbault), Paris, Dalloz, 2006, pp. 104 et s.

recopier[410]. Cette méthode réduit fortement le débat démocratique portant sur les questions traitées dans la directive.

C'est ce qui s'est d'ailleurs produit en Belgique. Depuis sa modification par la loi du 11 décembre 1998, la loi du 8 décembre 1992 copie littéralement la directive 95/46. Rares et minimes sont les éléments ajoutés ou modifiés par le législateur belge. Ce constat a été dénoncé par la section de législation du Conseil d'État qui qualifie de « carence coupable »[411], le manque de précisions apportées à la directive 95/46. Cette dernière est, à dessein, assez vague. Rappelons que l'objectif qu'elle poursuit est d'instaurer, dans les États-membres, un niveau de protection minimal applicable aux traitements de données[412], pour améliorer la circulation des données au sein de l'Union européenne. La directive établit donc des règles que les États doivent transposer pour atteindre ce résultat.

Pour ce faire, les États ne doivent pas reprendre littéralement les dispositions de la directive dans leur législation interne. « Transposer n'est pas copier »[413]. En l'occurrence, la copie des dispositions de la directive engendre « une insécurité juridique démesurée »[414]. Pour pallier à ce problème, il revient aux États d'adopter, dans leur ordre interne, des mesures de protection qui ne peuvent se réduire à des règles générales. En effet, « dans le système juridique de la Belgique, il ne suffit pas qu'une loi énonce un objectif général pour que celui-ci se réalise, le législateur qui doit veiller à cette réalisation doit indiquer les moyens que les diverses autorités auront à respecter pour y parvenir, ainsi que les règles que les sujets de droit auront à observer, à cette fin »[415].

---

410 *Idem ;* M. Delmas-Marty, *Pour un droit commun,* Paris, Seuil, 1994, p. 55 ; X. Bioy et P. Raimbault, « La puissance de la Loi en question », *in La puissance publiqu à l'heure européenne* (dir. P. Raimbault), Paris, Dalloz, 2009, pp. 105 et 116.

411 SLCE, avis du 2 février 1998 relatif à un avant-projet de loi « transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *op. cit.*, p. 174.

412 Voy. *supra*, n°s 65.- et s.

413 SLCE, avis du 2 février 1998 relatif à un avant-projet de loi « transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *op. cit.*, p. 174.

414 CPVP, avis n° 30/96, *op. cit.,* p. 3, n° 2.

415 SLCE, avis du 2 février 1998 relatif à un avant-projet de loi « transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *op. cit.*, p. 174.

Dans le troisième chapitre de cette partie de la recherche, on propose des solutions pour encadrer l'e-gouvernement sans se contenter de règles qui copient la directive 95/46[416].

§2. La complexité de l'accès à la loi et du contenu de celle-ci

96.- Considérations générales. Les démarches nécessaires pour accéder aux normes applicables à des traitements de données et ensuite les comprendre sont parfois très complexes. Elles peuvent d'ailleurs pousser à la mauvaise humeur voire au découragement des chercheurs universitaires dont le travail quotidien est pourtant consacré à l'étude de cette matière au sein d'un centre de recherches spécialisé dans ce domaine. On a peine à croire qu'un citoyen souhaitant simplement prendre connaissance de l'environnement juridique qui l'entoure y parviendrait plus aisément…

97.- La difficulté d'accéder aux règles. La législation applicable à l'e-gouvernement est embroussaillée, comme l'a déjà laissé percevoir l'exposé des règles nouvelles dans le chapitre introductif. Pour cette raison, il est difficile d'en prendre connaissance.

D'une part, il y a la *loi du 8 décembre 1992* relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[417], qui s'applique à tous les traitements de données[418], qu'ils soient effectués dans le secteur public ou le secteur privé.

D'autre part, des *lois dites « sectorielles »*, de plus en plus nombreuses, mettent en place un outil de traitement de données particulier, et prévoient, ci et là, des règles relatives à la protection de la vie privée des personnes concernées par celui-ci.

> La loi du 8 août 1983 sur le Registre national[419] et la loi du 15 janvier 1991 sur la Banque-Carrefour de la sécurité sociale[420] sont antérieures à la loi du 8 décembre 1992.

---

[416] Voy. *infra,* n°s 174.- et s.

[417] Rappelons que cette loi a été modifiée en 1998, suite à la transposition, en droit belge, de la directive 95/46 du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[418] Art. 3, al. 1er, de la loi du 8 décembre 1992.

[419] Loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.*, 21 avril 1984.

[420] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.,* 22 février 1990.

> Les autres sont plus récentes, qu'il s'agisse de la loi du 16 janvier 2003 sur la Banque-Carrefour des entreprises[421], la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules[422] ou encore la loi du 14 avril 2011 portant des dispositions diverses qui institue la Banque-Carrefour des permis de conduire[423].

À ces lois sectorielles s'ajoutent des *normes adoptées par les autorités fédérées*. On pense notamment au décret flamand du 8 mai 2009 relatif au Fichier central d'Adresses de Référence[424]. Le décret flamand du 18 juillet 2008 relatif à l'échange de données administratives[425] a une portée plus générale, ne visant pas un outil en particulier mais organisant, comme son nom l'indique, l'échange des données entre les administrations flamandes. La Communauté française et la Région wallonne ont également adopté un décret semblable[426].

Il existe aussi nombre d'*arrêtés royaux et gouvernementaux* précisant ces lois et ces décrets sans oublier la multitude d'*avis de la Commission de la protection de la vie privée* bien souvent nécessaires pour comprendre l'interprétation à donner à certaines notions particulièrement floues.

Les *décisions des comités sectoriels* ne doivent pas non plus être ignorées. Elles permettent de découvrir l'existence de certains outils de traitement, tels que l'entrepôt de données OASIS qui n'a aucune base légale ni réglementaire, n'étant organisé que par des décisions de comités sectoriels. En outre, puisque les comités sectoriels sont chargés d'autoriser les échanges de données entre les administrations, leurs décisions permettent de savoir concrètement quelle administration a accès à quelle donnée[427].

> L'utilisation des données au sein du réseau de la Banque-Carrefour de la sécurité sociale illustre la difficulté que représente l'accès aux normes.

---

[421] Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre du commerce, création de guichets-entreprises agréés et portant diverses dispositions, *M.B.*, 5 février 2003.

[422] Loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules, *M.B.*, 28 juin 2010.

[423] Loi du 14 avril 2011 portant des dispositions diverses, *M.B.*, 6 mai 2011.

[424] Decreet betreffende het Centraal Referentieadressenbestand, *M.B.*, 1er juillet 2009.

[425] Decreet betreffende het elektronische bestuurlijke gegevensverkeer, *M.B.*, 29 octobre 2008.

[426] Décret du 4 juillet 2013 portant assentiment à l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.*, 23 juillet 2013.

[427] C'est utile si on veut connaître, à l'avance, l'utilisation qui sera faite des données communiquées aux institutions de sécurité sociale ou si, *a posteriori*, on souhaite retracer le parcours d'une donnée pour vérifier si l'administration pouvait légalement y avoir accès, ou connaître l'origine d'une erreur affectant une information.

Prenons le cas d'un citoyen désirant connaître à l'avance l'utilisation qui sera faite des données qu'il communique à une institution de sécurité sociale telle que sa mutuelle.

Première difficulté : qu'est-ce qu'une institution de sécurité sociale ? La loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale est applicable aux « institutions de sécurité sociale ». Pour connaître celles-ci précisément, le citoyen ne peut se contenter de se référer à la définition donnée par la loi. Il doit également prendre connaissance des arrêtés royaux qui modifient cette notion[428]. Or, en allant sur le site www.moniteur.be, en sélectionnant « arrêté royal » et en indiquant « loi du 15 janvier 1990 – article 2 – sécurité sociale », on accède à 145 textes parmi lesquels il y a encore lieu d'identifier ceux qui portent éventuellement sur l'extension de la notion de sécurité sociale.

Deuxième difficulté : quelles sont les données enregistrées dans chaque institution de sécurité sociale ? Pour le comprendre, le citoyen doit disposer d'une vue d'ensemble des sources authentiques existant au sein du réseau de la sécurité sociale. Aucune norme ne prévoit un tel panorama.

Troisième difficulté : selon quelles règles sont échangées les données au sein de la Banque-Carrefour de la sécurité sociale ? Pour obtenir une réponse à cette question, le citoyen doit donc analyser l'ensemble des décisions du Comité sectoriel chargé de les autoriser. Est-ce raisonnablement possible ? On en doute. Rien qu'en 2010, le Comité sectoriel de la sécurité sociale et de la santé a rendu pas moins de 82 autorisations d'échanges de données. Plusieurs années de recherches menées par un juriste spécialisé en protection des données à caractère personnel permettraient difficilement de reconstituer un tableau exhaustif des données disponibles au sein du réseau sectoriel de la sécurité sociale et échangées entre les différents acteurs. Comment, dans ces conditions, considérer que l'obligation de garantir au citoyen l'accès aux normes et la prévisibilité des règles organisant des ingérences dans sa vie privée est respectée ?

98.- La difficulté de comprendre les règles. Ayant accédé aux normes, encore faut-il en comprendre le sens. Les tentatives de compréhension de la matière se heurtent bien souvent à un problème d'articulation entre les normes et à un problème de rédaction de celles-ci.

En particulier, *l'articulation* entre les lois et décrets sectoriels, d'une part, et la loi, générale, du 8 décembre 1992, d'autre part, se laisse difficilement appréhender. Ainsi, parmi les normes sectorielles, certaines mentionnent explicitement que la loi du 8 décembre 1992 doit être respectée. D'autres ne le prévoient pas. Pour les premières, la difficulté est de savoir quelle loi appliquer en cas de contradiction entre elles. Pour les secondes, on ne sait

[428] Art. 2, dernier al., de la loi du 15 janvier 1990.

si ce silence signifie que la loi du 8 décembre 1992 ne s'applique pas ou, au contraire, s'applique par défaut[429].

> Par exemple, la loi portant création d'une Banque-Carrefour des véhicules prévoit que « sans préjudice des dispositions de la présente loi, la loi du 8 décembre 1992 [...] s'applique aux donnés à caractère personnel visées dans la présente loi ». Elle précise que « en cas de contradiction entre les dispositions de la présente loi et celles de la loi du 8 décembre 1992 [...], c'est la réglementation la plus favorable à la protection de la vie privée des personnes physiques qui s'applique »[430]. Néanmoins, comment identifier la « réglementation la plus favorable » ? À ce propos, on regrette que l'avis de la section de législation du Conseil d'État n'ait pas été suivi. Il y était soutenu que « l'exposé des motifs gagnerait à être complété par un tableau qui mentionne d'une part, les dispositions qui seraient le cas échéant plus exigeantes que les garanties prévues par la loi du 8 décembre 1992 précitée et d'autre part, par les dispositions qui constitueraient un allègement ou des dérogations aux mêmes garanties données par cette loi »[431].

Quant à la *rédaction* des normes encadrant l'e-gouvernement, elle souffre de ce que l'informatique implique l'usage d'un jargon nouveau créé au rythme de l'apparition des nouveaux outils à réglementer. Leur sens est d'autant plus difficile à saisir que, bien souvent, ces notions nouvelles ne font pas l'objet d'une définition claire. En outre, on sent parfois le législateur dépassé par sa tâche, si bien que nombre de normes sont imprécises ou lacunaires et freinent, voire empêchent, la compréhension de la matière. Il en résulte un « manque de terminologie précise, l'absence de définitions nettes, la déficience de l'enchaînement logique des énoncés, l'abandon de l'économie de mots au profit du verbalisme d'un jargon technocratique de mauvais aloi »[432].

Face à de telles difficultés, on doute que les normes encadrant l'e-gouvernement soient suffisamment intelligibles pour satisfaire à l'exigence de prévisibilité de l'article 22 de la Constitution.

> La loi du 8 décembre 1992 et les normes sectorielles font peser nombre d'obligations sur le « responsable du traitement ». C'est à lui, par exemple, que peut s'adresser une personne désirant savoir si l'administration a enregistré

[429] Pour une ébauche de solutions possibles à partir des règles classiques en matière de conflits de lois voy. D. De Bot, *Verwerking van persoonsgegevens*, Anvers, Kluwer, 2001, pp. 11 et s. et références citées.

[430] Art. 3 de la loi portant création de la Banque-Carrefour des véhicules.

[431] SLCE, avis n° 47.162/4, du 2 décembre 2009 sur un avant-projet de loi portant création de la Banque-Carrefour des véhicules, *Doc. Parl.,* Chambre, session 2009-2010, n° 52-2493/001, p. 39.

[432] J.-P. Quéneudec, *op. cit.*, p. 1321.

des données à son sujet et à qui elle est susceptible de les transmettre. Mais qui est concrètement le responsable du traitement au sein d'une administration ? La loi ne le dit pas.

Les administrations doivent, en principe, obtenir l'autorisation du comité sectoriel compétent pour pouvoir accéder à des données détenues par une autre administration. Mais qui est le comité sectoriel compétent ? Quelle est la procédure à suivre pour introduire la demande d'autorisation ? Selon quels critères celle-ci est-elle accordée ou refusée ? Ce sont autant de questions qui trouvent difficilement réponse dans les normes applicables à l'e-gouvernement.

On ne compte plus les concepts imprécis et indéterminés qui jalonnent l'e-gouvernement. Le régime juridique censé encadrer l'utilisation des technologies s'articule sur les notions de « source authentique de données », de « plateforme d'échange d'informations », de « Banque-Carrefour », de « réseau », d' « intégrateur de services, d' « intégrateur de données », etc. À ces concepts s'ajoutent des abréviations exotiques désignant certaines bases de données, tels qu'OASIS, GENESIS, DIMONA, etc. La compréhension de ces concepts peu ou pas définis est complexe, surtout pour un juriste.

II. La densité de l'exigence de légalité dans l'e-gouvernement

99.- Deux impératifs. Ainsi qu'on l'a montré par divers exemples, organiser l'e-gouvernement n'est pas une chose aisée. L'encadrement normatif de cette matière est tiraillé entre deux impératifs. D'un côté, en vertu de l'article 22 de la Constitution, une loi est nécessaire pour organiser les traitements de données à caractère personnel effectués dans l'administration. D'un autre côté, la législation en matière d'e-gouvernement est tributaire de contraintes liées au fonctionnement de l'administration. Celles-ci s'opposent à ce que le législateur se montre trop invasif en réglant chaque traitement de données dans le moindre détail.

En définitive alors, parmi les aspects de l'e-gouvernement à encadrer, quels sont ceux qui doivent être déterminés par le législateur, et ceux qui peuvent être laissés à la discrétion du Roi ? Les lignes qui suivent sont consacrées à ces questions.

A. L'intervention du législateur

100.- Le contenu de la loi. Le législateur est soumis au respect de l'article 22 de la Constitution lorsqu'il organise un traitement de données à caractère personnel. Doit-il également respecter l'ensemble des normes qui constituent le régime juridique de la protection des données à caractère personnel ?

À cet égard, la jurisprudence de la Cour constitutionnelle est empreinte d'hésitations. À trois reprises[433], la Cour constitutionnelle a été amenée à se prononcer sur la constitutionnalité, au regard de l'article 22 de la Constitution, d'une norme de valeur législative organisant un traitement de données à caractère personnel. Elle s'est ainsi prononcée, en 2000, sur la constitutionnalité d'une loi créant un Centre d'information et d'avis sur les organisations sectaires nuisibles[434], en 2008, sur la constitutionnalité d'un décret flamand relatif au système d'information santé dont il a déjà été question plus haut[435] et, en 2010, sur la constitutionnalité d'une loi relative à l'institution et à l'organisation de la plate-forme *eHealth*[436]. Ces arrêts sont analysés ci-après.

Deux solutions ont été successivement appliquées par la Cour constitutionnelle.

La première solution consiste à soumettre le législateur à la loi du 8 décembre 1992. Cette solution est critiquable. Elle a pourtant été appliquée par la Cour constitutionnelle dans ses deux premiers arrêts.

La deuxième solution consiste en une lecture conciliante de l'article 22 de la Constitution et des normes internationales organisant la protection des données à caractère personnel. Cette solution plus orthodoxe a été appliquée par la Cour dans son troisième arrêt.

§1. La soumission des normes de valeur législative à la loi du 8 décembre 1992

101.- Une méthode critiquable. Dans l'arrêt rendu en 2000 et l'arrêt rendu en 2008 portant tous deux sur la constitutionnalité d'une norme de valeur législative organisant un traitement de données à caractère

[433] Nous n'analysons que les affaires soumises à la Cour constitutionnelle dans lesquelles les requérants ont invoqué des arguments tirés du régime juridique de la protection des données à caractère personnel. C'est la raison pour laquelle nous n'analysons pas, notamment, les arrêts rendus en 2013 au sujet de certaines lois fiscales (il s'agit des arrêts n° 06/2013 précité ; n° 18/2013, du 21 février 2013 ; n° 54/2013, du 18 avril 2013 ; n° 66/2013 précité). Bien que ces lois impliquent des traitements de données à caractère personnel, les requérants n'ont malheureusement pas invoqué le régime juridique de la protection des données à caractère personnel.

[434] C.C. arrêt n° 31/2000, du 21 mars 2000.

[435] C.C., arrêt n° 15/2008, du 14 février 2008.

[436] C.C., arrêt n° 29/2010, du 18 mars 2010. La plateforme *eHealth* est une institution publique chargée d'organiser l'échange sécurisé de données à caractère personnel relatives à la santé entre les acteurs des soins de santé.

personnel[437], la Cour constitutionnelle vérifie que la norme attaquée respecte la loi du 8 décembre 1992.

> Par exemple, dans l'arrêt rendu en 2000, la Cour se contente de vérifier que la loi attaquée ne contredit pas la loi du 8 décembre 1992. En d'autres termes, elle s'assure que les règles particulières prévues par la loi attaquée ne portent pas « atteinte aux garanties prévues par la loi attaquée » et ne constituent « que des garanties supplémentaires ». Son analyse la pousse à rejeter le moyen « en tant qu'il objecte que la loi attaquée entoure le traitement de données à caractère personnel par le Centre de moins de garanties que n'en prévoit le régime de droit commun »[438].

Deux critiques sont adressées à cette méthode.

a) La loi du 8 décembre 1992 comme garantie de constitutionnalité. En prônant une telle méthode, la Cour élève la loi du 8 décembre 1992 au rang de norme de référence par rapport à laquelle doit être confrontée la norme attaquée.

Or, confronter une norme de valeur législative à une loi non répartitrice de compétence heurte l'article 142 de la Constitution et les règles de la loi spéciale du 6 janvier 1989[439] qui déterminent strictement la compétence de la Cour constitutionnelle. En effet, sur la base de ces dispositions, la haute juridiction doit déclarer irrecevables les moyens qui dénoncent directement la violation d'une norme de valeur législative. Seules les règles – constitutionnelles et législatives – répartitrices de compétence et les droits fondamentaux contenus dans le Titre II de la Constitution peuvent servir de normes de référence[440].

b) La loi du 8 décembre 1992 comme garantie de prévisibilité. La Cour semble considérer que le respect de la loi du 8 décembre 1992 suffit à rendre la norme prévisible, comme l'exige l'article 22 de la Constitution. La méthode prônée par la Cour constitutionnelle est donc fondée sur le postulat que la loi du 8 décembre 1992 est suffisamment complète et prévisible pour encadrer tous les traitements de données. Or, tout au plus la loi du 8 décembre 1992 indique-t-elle les exigences à atteindre de manière abstraite mais elle ne les concrétise pas au cas par cas. On conçoit donc difficilement que la loi du 8 décembre 1992 soit suffisamment précise pour prétendre encadrer tous les traitements de données particuliers.

---

[437] C.C., arrêt n° 31/2000, du 21 mars 2000 ; C.C., arrêt n° 15/2008, du 14 février 2008.

[438] C.C., arrêt n° 31/2000, du 21 mars 2000, *op. cit.*, B.5.5.

[439] Loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, *M.B.*, 7 janvier 1989, p. 315.

[440] Voy. not., M.-F. Rigaux et B. Renauld, *op. cit.*, p. 97, et les références citées ; M. Verdussen, *Justice constitutionnelle*, Bruxelles, Larcier, 2012, pp. 86 à 101.

Par exemple, dans son arrêt de 2008, la Cour se prononce sur la précision quant à la nature des données utilisées dans le système information santé réglé par le décret flamand attaqué. Ce décret prévoit, en effet, que « le dossier de santé individuel contient au moins les données suivantes » et dresse une liste de cinq données, cette liste pouvant être complétée par le Gouvernement flamand. Pour juger de la précision d'une telle liste, la Cour se réfère exclusivement aux travaux préparatoires qui, pour indiquer le sens à donner à cette énumération exemplative, se référaient uniquement à l'article 4 c) de la loi du 8 décembre 1992, et n'exigeaient pas d'autre précision quant aux types de données effectivement utilisées. À nouveau, peut-on raisonnablement considérer qu'un citoyen est à même de connaître, à la lecture de cette disposition, les données exactes qui seront traitées à son sujet ? Quand bien même il voudrait se référer aux travaux préparatoires du décret, faudrait-il encore qu'il puisse y accéder. Quand bien même il aurait franchi ces deux étapes, il ne trouverait dans ces textes que la répétition d'une exigence abstraite figurant dans la loi du 8 décembre 1992, à savoir que « les données personnelles doivent être suffisantes, pertinentes et non excessives ». Comment considérer que les citoyens ont, à partir de telles dispositions, une connaissance claire des traitements de données à caractère personnel les concernant ?

En outre, dans une telle hypothèse, on doit malheureusement constater que le législateur ne procède pas lui-même à l'examen de proportionnalité des données[441]. Les données utilisées ne sont pas énoncées par la norme, et sont laissées à la discrétion du pouvoir exécutif, bien qu'elles constituent un élément essentiel du traitement[442].

§2. La détermination des éléments essentiels du traitement

102.- L'article 22 de la Constitution comme norme de référence. Examiner la conformité des lois, décrets et ordonnances par rapport à la loi du 8 décembre 1992 heurte des exigences constitutionnelles, comme en font état les lignes qui précèdent. Il serait dès lors plus conforme au droit de confronter directement les normes de valeur législative à l'article 22 de la Constitution.

Néanmoins, on le devine, cette méthode souffre du caractère vague de l'article 22 de la Constitution[443]. On comprend dès lors le besoin de se

[441] Comme nous le verrons dans la suite de l'étude (voy. *infra,* n°s 136.- et s.), l'examen de proportionnalité des données suppose notamment de s'assurer que seules les données pertinentes et non excessives seront utilisées.

[442] Pour d'autres exemples, voy. E. Degrave et Y. Poullet, « La vie privée face aux technologies », *in Les droits fondamentaux en Belgique* (dir. M. Verdussen et N. Bonbled), *op. cit.,* pp. 1020 à 1023.

[443] Au sujet du caractère vague des droits fondamentaux en général, voy. H. Dumont et C. Horevoets, « L'interprétation des droits constitutionnels », *op. cit.,* pp. 151 et s.

référer à des exigences plus précises, propres aux traitements de données à caractère personnel. C'est pourquoi, il peut être judicieux d'enrichir l'interprétation de l'article 22 de la Constitution en recourant aux normes protégeant la vie privée face aux traitements de données à caractère personnel.

> On pense à la directive 95/46, à la Convention n° 108 et à l'article 8 de la Convention européenne des droits de l'homme tel qu'interprété par la Cour européenne des droits de l'homme dans plusieurs affaires relatives à des traitements de données.

Il s'agit de recourir à la méthode dite du « tout indissociable »[444] selon laquelle, lorsqu'une disposition conventionnelle trouve écho dans une ou plusieurs dispositions constitutionnelles, « les garanties consacrées par cette disposition conventionnelle constituent un ensemble indissociable avec les garanties inscrites dans les dispositions constitutionnelles en cause [...] Lorsqu'est alléguée la violation d'une disposition du titre II, la Cour tient compte, dans son examen, des dispositions de droit international qui garantissent des droits ou libertés analogues »[445]. « On est, de la sorte, dans une logique, non plus de hiérarchie, mais de circularité. Dans une perspective, non plus de concurrence, mais de complémentarité »[446]. La protection des droits fondamentaux consacrés par la Constitution est ainsi renforcée[447].

Dans l'arrêt *Ehealth* rendu le 18 mars 2010[448], la Cour constitutionnelle s'inscrit dans cette démarche. Contrairement aux arrêts rendus antérieurement en matière de protection des données que l'on vient d'évoquer, la Cour renonce ici à confronter la norme attaquée à la loi du 8 décembre 1992. Elle rappelle d'ailleurs que « rien ne s'oppose, en principe, à ce

---

[444] M. Verdussen, *Justice constitutionnelle*, *op. cit.*, pp. 132 et s.

[445] C.C., arrêt n° 136/2004, du 22 juillet 2004, B.5.3. et B.5.4. Voy. également P. Vanden Heede et G. Goedertier, « De doorwerking van het internationale recht in the rechtsprrak van het Arbitragehof », *in Doorwerking van international recht in de Belgische rechtsorde. Recente ontwikkelingen in ee rechtsakoverschrijdend perspectief* (dir. J. Wouters et D. Van Eeckhoutte), Anvers, Intersentia, 2006, pp. 239 à 294 ; J. Velaers, « De samenloop van grondrechten in het Belgische rechtsbestel », *in Samenloop van grondrechten in verschillende rechtsstelsels* (dir. A. Nieuwenhuis, L. Dragstra, J. Velaers, L. Huybrechts, H. Wolswijk, F. Salomons, B. de Groot et S. Voet), Den Haag, Boom Juridische uitgevers, 2008, pp. 81 à 141 ; H. Dumont et C. Hoorevoets, « L'interprétation des droits constitutionnels », *in Les droits fondamentaux en Belgique* (dir. M. Verdussen et N. Bonbled), *op. cit.*, pp. 192 à 198.

[446] M. Verdussen, « Introduction », *in La vie privée au travail,* Louvain-la-Neuve, Anthémis, 2011, p. 14.

[447] H. Dumont et C. Hoorevoets, *op. cit.*, p. 195.

[448] C.C., arrêt n° 29/2010 précité. Pour un commentaire de cet arrêt, voy. J. Herveg, « Note d'observations », sous C. C., 18 mars 2010, *R.D.T.I.,* 2010, pp. 38-52.

qu'une disposition de nature législative déroge à une autre disposition de même nature »[449].

Toutefois, dit-elle, « la Cour peut examiner si le législateur a respecté les obligations internationales qui découlent des dispositions invoquées de la directive précitée, de la Convention n° 108 précitée auxquelles la loi précitée du 8 décembre 1992 et ses modifications ultérieures donnent exécution ». Et d'ajouter que « ces obligations forment un tout indissociable des garanties qui sont reproduites à l'article 22 de la Constitution. Une disposition qui est contraire à ces obligations violerait par conséquent le droit au respect de la vie privée, tel qu'il est garanti à l'article 22 de la Constitution »[450].

En d'autres termes, pour vérifier la constitutionnalité d'une loi organisant un traitement de données, la Cour constitutionnelle confronte cette norme à l'article 22 de la Constitution et à certains éléments du régime juridique de la protection des données à caractère personnel. Ces éléments font l'objet du point suivant.

103.- La détermination des éléments à régler dans la loi. Il reste à savoir quels sont les éléments que doit déterminer le législateur pour respecter cet ensemble indissociable d'exigences. Doit-il organiser chaque traitement dans le moindre détail ?

a) L'arrêt Rotaru contre Roumanie de la Cour européenne des droits de l'homme. La solution s'origine dans un arrêt de la Cour européenne des droits de l'homme, l'arrêt *Rotaru*[451]. Cet arrêt est fondamental en matière de protection des données puisque la Cour européenne des droits de l'homme y définit les éléments qui, selon elle, doivent figurer dans la norme organisant le traitement de données à caractère personnel, afin d'assurer la prévisibilité de cette dernière.

> Cet arrêt concerne un citoyen roumain, Monsieur Rotaru, qui, après la chute du régime communiste, assigne notamment le Ministère de l'Intérieur pour obtenir réparation suite aux persécutions qu'il a subies avant la chute du régime. Pour sa défense, le Ministère produit, lors du procès, une lettre que lui a adressée le Service roumain de renseignements contenant des informations sur le passé de Monsieur Rotaru, parmi lesquelles certaines sont fausses. Monsieur Rotaru tente, en vain, d'obtenir la rectification de ces erreurs en épuisant les voies de recours internes. Il assigne alors la Roumanie devant la Cour européenne des droits de l'homme, arguant notamment du fait que le

[449] *Ibid.*, B.5.3.

[450] *Idem.*

[451] Cour eur D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000, Req. 28341/95, § 57, *R.T.D.H.*, 2001, pp. 137 et s., note O. De Schutter.

> Service roumain de renseignements « détient et peut utiliser à tout moment des données sur sa vie privée, dont certaines sont fausses et diffamatoires. Il allègue la violation de l'article 8 de la Convention »[452]
>
> Après avoir reconnu que l'article 8 de la Convention européenne des droits de l'homme s'applique à ce cas[453], la Cour européenne des droits de l'homme rappelle que les termes « prévues par la loi », contenus à l'article 8, §2, de la Convention européenne des droits de l'homme suppose une loi de qualité. Tel n'est pas le cas en l'espèce car la loi sur laquelle se fonde le Gouvernement pour justifier la légalité de l'ingérence dans la vie privée de Monsieur Rotaru « ne définit ni le genre d'informations[454] pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre. De même, ladite loi ne fixe pas de limite quant à l'ancienneté des informations détenues et la durée de leur conservation »[455]. La Cour relève également que ladite loi « ne renferme aucune disposition explicite et détaillée sur les personnes autorisées à consulter les dossiers, la nature de ces derniers, la procédure à suivre et l'usage qui peut être donné aux informations ainsi obtenues »[456]. Elle note aussi que, « bien que [ladite] loi habilite les autorités compétentes à autoriser les ingérences nécessaires afin de prévenir et contrecarrer les menaces pour la sécurité nationale, le motif de telles ingérences n'est pas défini avec suffisamment de précision »[457].
>
> Dans l'arrêt *Shimovolos v. Russia* rendu plus récemment et dont il a été question précédemment[458], la Cour européenne des droits de l'homme réitère des propos semblables. Elle affirme qu'une base de données détenue par les autorités publiques et contenant des informations sur les citoyens doit être encadrée par une loi fixant « the grounds for registration of a person's name in the database, the authorities competent to order such registration, the duration of the measure, the precise nature of the data collected, the procedures for storing and using collected data and the existing controls and guanrantees against abuse »[459].

À cet égard, la loi espagnole de protection des données est particulièrement intéressante. Elle consacre un chapitre particulier aux bases de données détenues par le secteur public et affirme que la création de tels fichiers suppose qu'une norme accessible détermine un certains nombre

---

452 § 41 de l'arrêt.
453 §§ 43 et 44 de l'arrêt.
454 C'est nous qui soulignons.
455 § 57 de l'arrêt.
456 *Idem.*
457 § 58 de l'arrêt.
458 Voy. *supra,* n° 89.-
459 Cour eur. D.H., arrêt *Shimovolos v. Russia,* 21 juin 2011, Req. 30194/09, § 69.

d'éléments relatifs aux traitements de données, semblables à ceux énoncés par la Cour européenne des droits de l'homme.

Ainsi est-il affirmé que :

"1. Files of the public administrations may only be created, modified or deleted by means of a general provision published in the Boletín Oficial del Estado or in the corresponding official gazette.

2. The provisions or the creation or modification of files must indicate :

a) The purpose of the file and its planned use.

b) The persons or bodies on which it is planned to obtain personal data or which they are obliged to submit data.

c) The procedure for collecting the personal data.

d) The basic structure of the file and a description of the personal data included in it.

e) The intended transfers of personal data and, where applicable, the intended transfers of data to third countries.

f) The officials in the administrations responsible for the file.

g) The services or units with which the rights of access, rectification, cancellation and objection may be exercised.

h) The security measures, indicating the basic, medium or high level required"[460].

b) La jurisprudence de la Cour constitutionnelle et de la section de législation du Conseil d'État. La Cour constitutionnelle et la section de législation du Conseil d'État s'inspirent de la jurisprudence de la Cour européenne des droits de l'homme dans leurs propres décisions, ce qui les amène à soutenir que le législateur doit déterminer les « éléments essentiels du traitement »[461] et à identifier ceux-ci. Ces éléments concernent de multiples aspects d'un traitement de données à caractère personnel.

Ainsi, le législateur doit définir lui-même les *données* utilisées et leur *mode de collecte*[462].

---

[460] Art. 20 de la *Ley Orgánica de Protección de Datos de Carácter Personal de España* du 13 décembre 1993, dans sa traduction anglaise disponible sur le site de l'autorité espagnole de protection des données http://www.agpd.es

[461] Voy. not. C.C., arrêt n° 202/2004, *op. cit.*, B.6.2. et B.6.3.

[462] Avis L. 37.765/1/2/3/4 du 4 novembre 2004 sur un avant-projet de loi-programme, *Doc. Parl.*, Chambre, 2004-2005, n° 1437, p. 634 ; avis L. 41.662/1/2/3/4 des 14, 16 et 17 novembre 2006 sur un avant-projet de loi-programme (I), *Doc. Parl.*, Chambre, 2006-2007, n° 2773/1, p. 425 ; avis L. 40.079/2 du 12 avril 2006 sur un avant-projet de loi portant assentiment au Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume

L'*objectif* poursuivi par le traitement[463], appelé également « finalité » du traitement, est un élément essentiel de celui-ci.

Il en va de même de la *durée de conservation* des données. Cela suppose que le législateur fixe au moins les délais maximum de conservation des données[464].

La *communication* des informations, dite aussi « réutilisation » doit également être organisée par le législateur lui-même[465].

---

des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, et aux annexes, faits à Prüm le 27 mai 2005, *Doc. Parl.,* Chambre, 2005-2006, n° 2645/1, cité par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2006 », *op. cit.,* p. 280 ; avis L. 27.289/4 du 25 février 1998 sur un avant-projet de loi relatif à la sécurité lors des matches de football, *Doc. Parl.,* Ch. Repr., 1997-1998, n° 1572/1, p. 50 ; avis L. 42.774/3 et L. 42.775/3 du 24 avril 2007 sur 1. un projet d'arrêté royal fixant les règles relatives aux missions, à la gestion et à l'exploitation de Be-Health (42.774/3), et 2. un projet d'arrêté royal « relatif à la gestion financière de Be-Health, en tant que Service de l'État à gestion séparée » (42.775/3), cité par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2007 », *op. cit.,* p. 239 ; avis L. 47.162/4, *op. cit.*, p. 43.

[463] C.C., arrêt n° 15/2008 du 14 février 2008, B. 22 ; C.C., arrêt n° 29/2010, *op. cit.,* B.11 et s ; C.C., arrêt n° 1/2011 du 13 janvier 2011, pp. 28 et 29, B.12.1 et s. ; avis L. 41.662/1/2/3/4 des 14, 16 et 17 novembre 2006 sur un avant-projet de loi-programme (I), *op. cit.,* p. 425 ; avis L. 38.782/2/V du 11 août 2005 sur un avant-projet de loi relative à l'analyse de la menace, *Doc. Parl.,* Chambre, 2005-2006, n° 2032/1, p. 64.

[464] Avis L. 37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc. Parl.,* Chambre, 2004-2005, n° 1598/1 et 1599/1, cité par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2004 », *op. cit.,* p. 261.

[465] Avis L. 29.125/4 du 14 avril 1999 sur un projet d'arrêté royal réglant les modalités de la gestion des billets à l'occasion des matches de football, cité par R. Andersen et P. Nihoul, « Le Conseil d'État. Chronique de jurisprudence 1999 », *R.B.D.C.,* 2000/3-4, p. 354 ; avis L. 37.765/1/2/3/4 du 4 novembre 2004 sur un avant-projet de « loi-programme », *Doc. Parl.,* Chambre, 2004-2005, n° 1437, *op. cit.,* p. 261 ; avis L. 27.289/4 du 25 février 1998 sur un avant-projet de loi relatif à la sécurité lors des matches de football, *op. cit.*, p. 46 ; avis L. 43.186/3 du 19 juin 2007 sur un avant-projet de décret « over de jeugbijstand », *P.D.G.,* 2007-2008, n° 120/1 et avis L. 43.489/4 du 10 décembre 2007 sur avant-projet de décret relatif à l'information, la coordination et l'organisation des chantiers sous, sur ou au-dessus des voiries ou des cours d'eau, *Doc. Parl. W.,* 2008-2009, n° 913/1, cités par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2007 », *op. cit.,* p. 239 ; avis L. 42.064 du 24 janvier 2007 sur un avant-projet de loi « relatif à certains traitements de données à caractère personnel par le Service Public Fédéral Finances », *Doc. Parl.,* Ch. Repr., n° 52-3064/1, cité par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2007 », *op. cit.,* p. 240. Cet avis précise qu'une « simple autorisation d'un comité sectoriel ne saurait suffire » pour organiser « la communication de données à caractère personnel par le SPF Finances à des professions ou des États étrangers ».

Par ailleurs, le législateur doit mentionner les *personnes autorisées* à consulter une base de données ainsi que les *conditions* de cette consultation[466].

Enfin, le législateur peut instituer des *autorités de contrôle*, appelées « comités sectoriels », chargées d'autoriser, ou non, les traitements de données, à la condition d'encadrer leur pouvoir de décision en prévoyant lui-même les critères devant guider les autorisations accordées[467].

104.- Une solution encourageante. La solution dégagée par la Cour européenne des droits de l'homme et relayée par la Cour constitutionnelle et la section de législation du Conseil d'État est particulièrement intéressante dans le contexte de l'e-gouvernement. Rappelons[468], en effet, que les données traitées par les administrations sont des informations personnelles que les citoyens ont été contraints de donner. Il importe donc que l'utilisation de ces données soit balisée de manière claire, par le législateur.

Comme on l'a dit précédemment, l'intervention du législateur à propos des éléments essentiels du traitement de données permet qu'un débat démocratique soit mené au sujet des paramètres les plus importants d'une telle ingérence dans la vie privée. Dans le même temps, on ne laisse pas la détermination de ces aspects des traitements de données à la discrétion des administrations qui risqueraient de donner trop de poids à l'efficacité administrative par rapport à la protection de la vie privée des citoyens.

Par ailleurs, le fait, pour le législateur, de centrer son travail sur les aspects essentiels des traitements de données aide à la clarté des règles, mais leur donne également une force particulière. Comme l'affirme Bertrand Mathieu, « le recentrage du législateur sur les règles et principes les plus importants ne peut que renforcer son rôle. En effet, le juge de la loi

---

[466] Avis L. 43.186/3 du 19 juin 2007 sur un avant-projet de décret « over de jeugbijstand », P.D.G., 2007-2008, n° 120/1 et avis L. 43.489/4 du 10 décembre 2007 sur avant-projet de décret relatif à l'information, la coordination et l'organisation des chantiers sous, sur ou au-dessus des voiries ou des cours d'eau, *Doc. Parl. W.,* 2008-2009, n° 913/1, cités par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2007 », *op. cit.,* p. 239.

[467] Avis L. 33.962/2 du 19 novembre 2002 sur un avant-projet de loi « modifiant la loi du 8 août 19 83 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques », *Doc. Parl.,* Chambre, sess. 2002-2003, n° 2226/1, p. 51. Dans le même sens, à propos du C.S.A, l'avis n° 33.865/3 du 13 novembre 2002 sur un avant-projet de décret « sur la radiodiffusion », *Doc. CCF.,* sess. 2002-2003, n° 357/1, cité par R. Andersen, P. Nihoul el M. Joassart, « Le Conseil d'État. Chronique de jurisprudence 2002 », *op. cit.,* p. 86.

[468] Voy. *supra,* n° 62.-

[...] sera nécessairement plus prudent face à une disposition qui manifeste de la part du législateur une volonté claire et forte sur une question générale. Le principe qui s'oppose à la loi devra alors présenter une force et une clarté supérieure à celui que la loi exprime [...]. Ce n'est pas tant la force juridique qui sera ainsi garantie que sa force psychologique »[469].

105.- L'intérêt du régime juridique de la protection des données. Bien que les éléments essentiels du traitement, déterminés par les hautes juridictions, guident utilement la rédaction des lois encadrant l'e-gouvernement, des questions subsistent quant au contenu que le législateur doit leur donner, au cas par cas.

> Entre autres exemples, il revient au législateur de déterminer les données contenues dans une source authentique. Mais comment les choisir ? La réponse à cette question dépend notamment de l'objectif poursuivi par cette source authentique. En d'autres termes, la finalité du traitement, exigence du régime juridique de la protection des données, doit guider le législateur.
>
> Autre exemple. Le législateur doit organiser l'accès, par des administrations, à des données qu'elles n'ont pas collecté elles-mêmes. Vaut-il mieux mettre en place une base de données centralisée ou une plateforme d'échanges d'information ? Cette question renvoie à l'examen des risques que de tels outils représentent pour la protection de la vie privée des citoyens, et, partant, à l'exigence de proportionnalité, imposée par le régime juridique de le protection des données.

Pour déterminer le contenu de chaque élément essentiel d'un traitement particulier, le législateur doit être guidé par le régime juridique de la protection des données à caractère personnel et, en particulier l'exigence de finalité et l'exigence de proportionnalité. C'est l'objet du deuxième chapitre[470].

B. L'intervention du Roi

106.- E-gouvernement et pouvoir exécutif. Les développements qui précèdent montrent l'ampleur du rôle dévolu au législateur pour encadrer l'e-gouvernement. Est-ce à dire que l'intervention du Roi est réduite à néant ? Certainement pas. La Cour constitutionnelle et la section de législation du Conseil d'État invitent à ne pas interpréter de manière trop stricte l'exigence de légalité consacrée par l'article 22 de la Constitution.

---

[469] B. MATHIEU, *La loi, op. cit,* p. 131.
[470] Voy. *infra,* n°s 112.- et s.

> Elles affirment, en effet, que « les dispositions [...] de la Constitution qui réservent certaines matières à un législateur n'impliquent ni que le pouvoir exécutif ne puisse prendre aucune disposition les concernant ni que le législateur soit tenu de les régler en détail »[471]. En d'autres termes, « il n'est [...] pas requis que l'ensemble des éléments de la réglementation envisagée figure dans la loi »[472]. Soutenir le contraire reviendrait d'ailleurs à contraindre le législateur « à faire œuvre d'administration active, ce qui mettrait en cause l'efficacité des politiques qu'il arrête »[473].

Dès lors, les aspects de l'e-gouvernement qui ne doivent pas être déterminés par le législateur peuvent l'être par le Roi. Une double habilitation constitutionnelle le justifie. D'une part, les articles 37 et 107, alinéa 2, de la Constitution octroient au Roi la compétence exclusive d'organiser les services de l'administration générale. D'autre part, en vertu de l'article 108 de la Constitution, Il dispose d'un pouvoir réglementaire dérivé.

Néanmoins, il faut reconnaître que l'application de l'article 22 de la Constitution à l'e-gouvernement conduit à diminuer sensiblement l'intervention du Roi en cette matière.

§1. L'article 22 de la Constitution et le pouvoir du Roi d'organiser l'administration

107.- Les articles 37 et 107, alinéa 2, de la Constitution. En vertu de l'article 37 et de l'article 107, alinéa 2, de la Constitution, le Roi est compétent pour organiser les services de l'administration générale[474]. Le Roi est ainsi chargé de « créer des départements ministériels, des services au sein de ceux-ci, fixer les attributions des différents services, déterminer quels fonctionnaires peuvent prendre quelles décisions, instituer des organes collégiaux et préciser leur compétence [...] bref, organiser cette

[471] C.C., arrêt n° 189/2005, du 14 décembre 2005, B.10.3.

[472] P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2004 », *R.B.D.C.,* 2005/2, p. 260, n° 6 et les références citées.

[473] C.C., arrêt n° 189/2005, *op. cit.,* B.10.3. Voy. également SLCE, avis L. 34.547/AG du 11 février 2003 sur un projet d'arrêté royal « portant création d'une Commission *ad hoc* en ce qui concerne les avis négatifs relatifs aux candidats à un mandat au sein de l'Exécutif des Musulmans de Belgique », cité par P. Nihoul et M. Joassart, « Le Conseil d'État. Chronique de jurisprudence 2003 », *R.B.D.C.,* 2005/1, p. 50.

[474] F. Delpérée, *Le droit constitutionnel de la Belgique, op. cit.,* pp. 714-715, §§ 844 et 845 ; M. Uyttendaele, *Trente leçons de droit constitutionnel,* Bruxelles, Bruylant, 2011, p. 482 ; M. Leroy, *Les règlements et leurs juges,* Bruxelles, Bruylant, 1987, p. 63 ; J. Velaers, *De Grondwet en de Raad van State, afdeling wetgeving,* Maklu, Anvers, 1999, p. 369. Le pouvoir du Roi d'organiser les services de l'administration au sein des autorités fédérées se fonde sur l'article 87, §1, de la loi du 8 août 1980 de réformes institutionnelles.

masse énorme de moyens matériels et humains qu'est l'administration, c'est le rôle naturel du pouvoir exécutif »[475].

Or, chargé de définir les éléments essentiels de l'e-gouvernement, le législateur sera notamment amené à regrouper des institutions au sein de réseaux sectoriels et de définir les administrations responsables de sources authentiques de données[476]. Ces tâches empiètent sur la mission du Roi. Peut-on considérer que l'article 22 de la Constitution, qui fonde l'ample compétence du législateur, suffit à le justifier ?

108.- La réponse de la section de législation du Conseil d'État. Dans plusieurs avis, la section de législation du Conseil d'État freine les élans du législateur en rappelant la compétence du Roi d'organiser l'administration.

> À propos de l'octroi d'un pouvoir d'autorisation au Comité de direction institué au sein du SPF Finances, la section de législation soutient que « c'est au Roi que les articles 37 et 107, alinéa 2, de la Constitution confèrent le pouvoir de régler l'organisation des services publics fédéraux [...] Il en résulte que le législateur doit s'abstenir de s'immiscer dans l'organisation des services de l'administration générale »[477].
>
> La section de législation du Conseil d'État a repris littéralement cette justification dans son avis relatif au Cadastre de l'emploi non-marchand pour soutenir que le législateur ne pouvait attribuer au Secrétariat Général du Ministère de la Communauté française la mission de créer et de gérer un cadastre de l'emploi. Plutôt que de viser « le Secrétariat Général du Ministère de la Communauté française », le législateur devait désigner le Secrétaire général[478].

Toutefois, elle admet que le législateur peut s'immiscer dans la compétence du Roi d'organiser les services de l'administration, à la condition que cette immixtion soit justifiée par des « circonstances exceptionnelles » ou « des dispositions qui, en vertu de la Constitution, ne peuvent être édictées que par le législateur ».

Pour reprendre les termes de la section de législation du Conseil d'État, « cette immixtion n'est compatible avec la répartition constitutionnelle des compétentes entre les pouvoirs législatif et exécutif que si elle est justifiée par des circonstances exceptionnelles ou si elle concerne des dispositions qui, en vertu de la Constitution, ne peuvent être édictées que par le

[475] M. Leroy, *Les règlements et leurs juges*, *op. cit.*, p. 63.
[476] Voy. *infra*, n°s 175.-et s.
[477] S.L.C.E., avis n° 42.034/2, *op. cit.*, p. 10.
[478] SLCE, avis n° 42.243/2, *op. cit.*, p. 43.

législateur. Il convient dès lors que l'exposé des motifs justifie la nécessité de viser directement le Comité de direction dans la loi »[479].

Le respect de l'article 22 de la Constitution est-il une justification suffisante de l'immixtion du législateur dans les compétences du Roi ?

La réponse est affirmative. Elle a été donnée par la section de législation du Conseil d'État, chambre néerlandophone, dans l'avis rendu à propos du décret flamand relatif à l'échange électronique de données administratives.

Il ressort de cet avis que la protection de la vie privée doit primer sur la compétence du Roi. La section de législation du Conseil d'État constate que l'organisation de l'échange de données entre les administrations flamandes par l'instauration de sources authentiques de données et d'une plateforme d'échanges de données implique une immixtion du pouvoir législatif dans les services de l'administration, qui ressortit, en principe, de la compétence du gouvernement.

Elle affirme cependant qu'il doit être fait exception à ce principe dans la mesure où la protection de la vie privée est en jeu, et ce, en vertu de l'article 22 de la Constitution. Dans cette hypothèse, le législateur peut déterminer le cadre législatif applicable à l'administration et laisser au pouvoir exécutif le soin de le mettre en œuvre.

> La section de législation s'est prononcée en ces termes « In de mate dat het ontwerp betrekking heeft op de eigen diensten van de regering [...] gaat het in beginsel om een aangelegenheid tot de bevoegdheid van de Vlaamse Regering behoort, behoudens in zoverre het gaat om de bescherming van het recht op eerbiediging van het privé-leven. Dat laatste is op grond van artikel 22 van de Grondwet een aan de decreetgever voorbehouden aangelegenheid »[480].

L'application de l'article 22 de la Constitution conduit donc, concrètement, à une diminution importante de la compétence du Roi d'organiser aujourd'hui l'administration.

---

[479] *Ibid.,* p. 10. Ce tempérament est repris littéralement dans l'avis n° 42.243/2, *op. cit.,* p. 43.

[480] SLCE, avis n° 44.192/1 du 1er avril 2008 « over een voorontwerp van decreet 'betreffende het elektronische bestuurlijke gegevensverkeer' », *Doc. Parl.,* Parl. fl., session 2007-2008, n° 1712, pp. 129-130.

§2. L'article 22 de la Constitution et le pouvoir du Roi d'exécuter la loi

109.- L'article 108 de la Constitution. Le Roi dispose d'un pouvoir réglementaire dérivé, consacré par l'article 108 de la Constitution[481], en vertu duquel « le Roi est réputé compétent pour dégager du principe de la loi et de son économie générale les conséquences qui en dérivent naturellement d'après l'esprit qui a présidé à sa conception et les fins qu'elle poursuit, à condition que, ce faisant, le Roi n'étende pas la portée de la loi, ni ne la restreigne »[482].

Cela signifie que les mesures d'exécution de la loi adoptées sur la base de l'article 108 de la Constitution ne peuvent pas être « de nature à étendre ou à restreindre la portée de la loi »[483]. Dès lors, la loi doit être suffisamment précise afin que la compétence du Roi ne porte que sur « l'exécution de mesures dont les éléments essentiels sont fixés par le législateur »[484].

110.- Habilitations législatives et critères précis. Il résulte de cette interprétation de l'article 108 de la Constitution que le législateur doit encadrer le pouvoir d'exécution du Roi par des critères précis.

Par exemple, le législateur ne pourrait laisser au Roi le soin de déterminer lui-même d'autres données que celles énumérées par la loi. Dans la lignée de cette exigence, le Roi ne pourrait pas non plus déterminer

---

[481] F. Delpérée, *op. cit.,* p. 768. L'article 20 de la loi spéciale du 8 août 1980 octroie ce même pouvoir aux gouvernements des entités fédérées.

[482] Cass., 18 novembre 1924, *Pas.,* 1925, I, p. 25 ; Cass., 19 janvier 1959, *Pas.,* I, p. 494 ; Cass., 15 mars 1965, *Pas.,* I, p. 740 ; Cass., 5 mai 1970, *Pas.,* I, p. 766. Avis L. 39.514/1 relatif à un projet d'arrêté royal portant création et fixant la composition et les modalités de fonctionnement du Comité chargé de la qualité des données de la Banque-Carrefour des Entreprises et de son fonctionnement, du 29 novembre 2005, *M.B.,* 28 février 2006 ; avis L. 38.235/2 du 11 avril 2005 relatif à un projet d'arrêt royal déterminant les types d'information associés aux informations visées à l'article 3, al. 1er, de la loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.,* 25 janvier 2006 ; A. Alen, *op. cit.,* pp. 219 et 220 ; F. Delpérée, *op. cit.,* p. 768 ; R. Andersen et P. Nihoul, « Le Conseil d'État. Chronique de jurisprudence 1998 », *R.B.D.C.,* 2000/1, pp. 91 et 92.

[483] Avis L. 27.165/1 du 8 janvier 1998 sur un projet d'arrêté royal « portant des mesures d'exécution de la carte d'identité sociale », *M.B.,* 13 mars 1998.

[484] C.C., arrêt n° 95/2008, *op. cit.,* B.42 ; arrêt n° 29/2010, *op. cit.,* B.16. En ce sens également, avis L. 37.765/1/2/3/4 du 4 novembre 2004 sur un avant-projet de loi-programme, *Doc. Parl.,* Chambre, 2004-2005, n° 1437 ; avis L. 37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc. Parl.,* Chambre, 2004-2005, n° 1598/1 et 1599/1, cités par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2004 », *op. cit.,* p. 260.

les éléments fixant « la manière dont ces données seront traitées »[485] ni ajouter à la loi des objectifs qu'elle ne prévoit pas[486].

> Entre autres exemples, est définie en terme trop généraux, la compétence déléguée au Roi de « désigner certaines informations qui doivent être fournies lors de l'inscription dans la Banque-Carrefour des Entreprises » et d' « établir les liens avec les autres banques de données »[487].
>
> Doit être précisée, la disposition législative autorisant le Roi « à dresser la liste des informations qui doivent être communiquées à la banque de données et à déterminer les cas et les modalités de modification des informations »[488].

111.- Des mesures techniques. Outre l'exécution des éventuelles habilitations législatives encadrées par des critères précis, le rôle du Roi dans l'e-gouvernement peut consister à définir les mesures techniques des outils de traitement utilisés.

> Le Roi peut, par exemple[489], fixer les modalités de consultation[490] du cadastre des interconnexions de la Banque-Carrefour des véhicules.

La détermination des « types d'informations » relève également de la compétence du Roi. Un « type d'information » est une donnée qui livre à son utilisateur une compréhension plus exacte et à jour de l'information légale à laquelle elle est jointe[491]. En d'autres termes, si la donnée

---

[485] P. Nihoul, M. Joassart et V. franck, « Le Conseil d'État. Chronique de jurisprudence 2005 », *R.B.D.C.,* 2006/4, p. 413.

[486] Avis L. 38.782, *op. cit.,* p. 413 (à propos d'un avant projet de loi « relative à l'analyse de la menace) ; avis L. 40.079/2, *op. cit.,* p. 280 (à propos d'un avant-projet de loi portant assentiment d'un traité relatif à la coopération transfrontalière) ; avis L. 41.662/1/2/3/4, *op. cit,* p. 425 à propos d'une banque de données « Constitution de pensions complémentaires »).

[487] Avis L. 33.285/1, *op. cit.,* p. 103.

[488] Avis L. 41.662/1/2/3/4, *op. cit,* p. 425 (à propos d'une banque de données « Constitution de pensions complémentaires »).

[489] Dans le cadre de cette étude, nous ne ferons pas le relevé exhaustif de ces mesures techniques. Outre le fait que la lecture d'un tel relevé serait peu enthousiasmante, ce travail s'éloigne de l'objet du présent titre consacré au travail du législateur et de la démonstration réalisée dans la thèse.

[490] Art. 20 de la loi du 19 mai 2010.

[491] La notion de « type d'information » n'est pas définie par le législateur. Cette définition est créée à partir du Rapport au Roi relatif à l'arrêté royal du 8 janvier 2006 déterminant les types d'information associés aux informations visées à l'article 3, al. 1er, de la loi du 8 août 1983 sur le Registre national ainsi que des avis de la section de législation du Conseil d'État et des avis de la CPVP qui traitent de cette question. En ce qui concerne les *avis de la section de législation du Conseil d'État,* voy. Avis L. 38.235/2 relatif à un projet d'arrêté royal déterminant les types d'information associés aux informations visées à l'article 3, al. 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.,* 25 janvier

légale n'était pas accompagnée de la donnée technique, elle pourrait être interprétée erronément. Inversement, envisagée sans la donnée légale à laquelle elle est jointe, une donnée technique n'est pas compréhensible et ne présente pas d'intérêt pour les utilisateurs de la base de données qui la contient.

Actuellement, seules les données du Registre national sont précisées par des types d'informations. Ces derniers ont été ajoutés au Registre national par trois arrêtés royaux[492].

> Par exemple, la mention de la « plurinationalité » sous la donnée « nationalité » donne aux autorités une connaissance plus exacte de la nationalité de la personne concernée et leurs permet d'en tirer les conséquences administratives qui s'imposent dans ce cas.
>
> La mention du pseudonyme comme donnée technique de la donnée « nom » enregistrée au Registre national, « si elle n'est pas conforme à la lettre de la loi du 8 août 1983, est une conséquence qui dérive naturellement de son esprit » et peut donc être prévue par un arrêté royal[493].

*

2006 ; Avis L. 44.109/2 du 10 mars 2008 relatif à un projet d'arrêté royal modifiant l'arrêté royal du 8 janvier 2006 déterminant les types d'information associés aux informations visées à l'article 3, al. 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M B,* 28 mai 2008. *S'agissant des avis de la CPVP*, voy. CPVP, avis n° 12/2003 du 13 janvier 2003 sur un projet d'arrêté royal déterminant les informations techniques associées aux informations visées à l'article 3, al. 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques ; CPVP, avis n° 39/2003 du 25 septembre 2003 sur un projet d'arrêté royal déterminant les informations techniques associées aux informations visées à l'article 3, al. 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques ; CPVP, avis n° 24/2007 du 4 juillet 2007 sur un projet d'arrêté royal modifiant l'arrêté royal du 8 janvier 2006 déterminant les types d'information associés aux informations visées à l'article 3, alinéa 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques ; CPVP, avis n° 31/2007 du 7 novembre 2007 sur un projet d'arrêté royal modifiant l'arrêté royal du 8 janvier 2006 déterminant les types d'information associés aux informations visées à l'article 3, alinéa 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques ; avis n° 25/2008 du 2 juillet 2008 relatif au projet d'arrêté royal modifiant l'arrêté royal du 8 janvier 2006 déterminant les types d'information associés aux informations visées à l'article 3, alinéa 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques ; avis n° 01/2009 du 14 janvier 2009 concernant l'adaptation d'un code dans le type d'information relatif à l'état civil afin de prévenir les mariages de complaisance.

[492] Arrêté royal du 8 janvier 2006 précité ; Arrêté royal du 27 janvier 2008 modifiant l'arrêté royal du 8 janvier 2006 déterminant les types d'informations visées à l'article 3, alinéa 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.*, 20 février 2008 ; A.R. du 9 mai 2008 modifiant l'arrêté royal du 8 janvier 2006 déterminant les types d'information associés aux informations visées à l'article 3, alinéa 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.*, 28 mai 2008.

[493] Avis L. 38.235/2, *op. cit.*, § 2.1.

Conclusions

L'exigence de légalité est un pilier fondamental de l'État de droit. Elle est garantie par l'article 105 de la Constitution, en vertu duquel l'action administrative doit être encadrée par une loi au sens formel du terme. Puisqu'il implique des traitements de données à caractère personnel, l'e-gouvernement est également soumis à l'article 22 de la Constitution qui protège la vie privée des citoyens. Cette disposition constitutionnelle impose au législateur des obligations de légalité substantielle lorsqu'il organise un traitement de données à caractère personnel.

De par sa technicité et sa complexité, l'e-gouvernement ébranle l'exigence de légalité, et contribue au déclin de la loi. En effet, les normes qui encadrent les traitements de données au sein de l'administration sont multiples et éparses. Elles émanent de la collectivité fédérale, mais également des collectivités fédérées. En outre, certaines d'entre elles n'ont pas fait l'objet d'un réel débat démocratique. Par ailleurs, on peine bien souvent à les comprendre.

Partant de là, comment encadrer l'e-gouvernement en tenant compte, d'une part, de l'exigence de légalité, nécessaire à notre société démocratique, et, d'autre part, des contraintes de l'e-gouvernement qui s'opposent à une interprétation trop stricte de cette exigence ?

Dans un premier temps, nous avons identifié les législateurs qui, au sein de notre État fédéral, sont compétents pour organiser l'e-gouvernement. Il est apparu qu'aujourd'hui le législateur fédéral n'a plus le monopole s'agissant de l'organisation des traitements de données. Les normes en cette matière peuvent donc faire l'objet d'une loi, d'un décret ou d'une ordonnance. La Cour constitutionnelle et la section de législation du Conseil d'État imposent toutefois une limite de taille aux législateurs communautaires et régionaux, en les contraignant à respect la loi du 8 décembre 1992. Cette solution insatisfaisante a été critiquée.

Dans un deuxième temps, la tâche du législateur, à qui il revient d'encadrer l'e-gouvernement, a retenu notre attention. À quels critères peut-il se référer pour encadrer au mieux les traitements de données dans l'administration ? La formulation générale de l'article 22 de la Constitution le guide fort peu dans cette mission. Nous nous sommes alors tournés vers la jurisprudence de la Cour constitutionnelle et les avis de la section de législation du Conseil d'État, qui se sont prononcés à plusieurs reprises sur la mise en place de traitement de données.

Il est apparu que la première solution appliquée un temps par la Cour constitutionnelle, visant à soumettre toutes les normes, y compris législatives, à la loi du 8 décembre 1992, se heurte à des embûches juridiques.

Une autre solution est plus conforme au droit, qui consiste à recourir à la méthode du « tout indissociable » pour interpréter les lois, décrets et ordonnances au regard de l'article 22 de la Constitution, enrichi des textes internationaux et nationaux applicables aux traitements de données à caractère personnel. L'étude de la jurisprudence de la Cour constitutionnelle et de la section de législation du Conseil a révélé que seuls les éléments essentiels du traitement doivent être définis par le législateur. Le rôle du législateur est donc ample. Cela a des conséquences sur le rôle du Roi, qui n'est pas réduit à néant mais est diminué dans l'e-gouvernement.

Il n'en demeure pas moins que, malgré la mise en lumière des éléments essentiels du traitement, la tâche du législateur demeure assez floue. Par exemple, comment déterminer les données qui doivent figurer dans une base de données ? Comment choisir entre un numéro d'identification unique ou un numéro d'identification sectoriel ? Le législateur doit être guidé dans de tels choix. Le régime juridique de la protection des données à caractère personnel l'y aide, en organisant une exigence de finalité et une exigence de proportionnalité. Elles font l'objet du chapitre suivant.

*

CHAPITRE II.
L'e-gouvernement et les exigences de finalité et de proportionnalité des traitements de données à caractère personnel

Introduction

112.- Des obligations cardinales qui guident le législateur. Les exigences de finalité et de proportionnalité sont des obligations cardinales du régime de protection des données à caractère personnel[494].

Ces exigences découlent directement de l'article 8 de la Convention européenne des droits de l'homme selon lequel toute ingérence dans la protection de la vie privée doit poursuivre au moins un des objectifs repris au paragraphe 2 de cette disposition. C'est l'exigence de finalité. Cette ingérence doit être nécessaire pour la réalisation de cet objectif. C'est l'exigence de proportionnalité.

La finalité et la proportionnalité d'un traitement de données à caractère personnel font l'objet d'une riche interprétation de la part de la CPVP, dans des avis consacrés notamment au développement de l'e-gouvernement.

---

[494] S. Gutwirth, « De toepassing van het finaliteitsbeginsel », *T.P.R.,* 1993, II, pp. 1409 et s ; T. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995 », *J.T.*, 1999, p. 384 ; M.-H. Boulanger, C. de Terwangne et T. Léonard, « La protection de la vie privée à l'égard des traitements de données à caractère personnel – La loi du 8 décembre 1992 », *J.T.*,1993, p. 377 ; C. de Terwangne, « Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles », *Les petites affiches,* 2005, p. 40 ; H. Maisl, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », *in L'Administration électronique au service des citoyens* (dir. G. Chatillon et B. Du Marais), Bruxelles, Bruylant, 2003, p. 355 ; S. Gutwirth, *Privacy and the Information Age*, Boston, Rawman & Littlefield Publischers, 2001, pp. 96 et s. ; H. Graux et J. Dumortier, *Privacywetgeving in de praktijk,* Courtrai, UGA, 2009, p. 31.

Le plus souvent, l'exigence de finalité est désignée par le vocable « principe de finalité ». Nous préférons parler d' « exigence de finalité », pour mettre en évidence qu'il s'agit d'une règle précise imposée par le régime juridique de la protection des données.

Ainsi qu'on l'a dit dans le premier chapitre, l'article 22 de la Constitution exige du législateur qu'il détermine les éléments essentiels des traitements de données qu'il organise. Les exigences de finalité et de proportionnalité issues de l'article 8 de la Convention européenne des droits de l'homme et de la directive 95/46 le guident dans cette tâche et, ce faisant, aboutissent à améliorer la qualité des lois encadrant l'e-gouvernement tout en aidant le législateur à garder une certaine prise sur l'action de l'administration.

*

Section 1. L'exigence de finalité

113.- La notion. La finalité d'un traitement de données est l'objectif en vue duquel il est réalisé.

Le cumul de l'article 8 de la Convention européenne des droits de l'homme et de la directive 95/46 aboutit à exiger que la finalité d'un traitement soit légitime, déterminée et explicite. En outre, en cas de réutilisation des données, la finalité de la réutilisation doit être compatible avec celle de la collecte[495].

La finalité constitue « l'axe focal »[496] d'un traitement de données, puisqu'elle impose « le cadre dans lequel les diverses opérations de

[495] La Convention n° 108 prévoit, en son article 5, que « les données à caractère personnel faisant l'objet d'un traitement automatisé sont b) enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités » ; l'article 8 de la Charte des droits fondamentaux prévoit que les données doivent être « traitées [...] à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi » ; la directive 95/46 dispose que les données doivent être « b) collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités » et prévoit, en son article 7, 6 « principes relatifs à la légitimation des traitements de données ». Les exigences de la directive 95/46 sont reprises dans la loi du 8 décembre 1992. Pour une application de chacune de ces exigences à la diffusion de la jurisprudence sur internet, voy. C. DE TERWANGNE, « Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles », *op. cit.*, pp. 40 à 48.

[496] CPVP, avis n° 24/96 du 13 septembre 1996 relatif à la consultation des dossiers de la Police des Etrangers déposés aux Archives générales du Royaume, p. 5 ; CPVP, avis n° 32/2001 du 10 septembre 2001 relatif à l'organisation de la publicité cadastrale, p. 3. Sur l'importance de l'exigence de finalité compte tenu de sa fonction d'encadrement des traitements de données, voy. également la thèse de R. DUASO CALÈS, *Principe de finalité,*

traitement peuvent avoir lieu »[497]. *In fine,* elle doit permettre « d'apprécier facilement et valablement la pertinence et la proportionnalité des données collectées »[498].

114.- La raison d'être. L'attention portée à cette exigence s'explique par les risques induits lorsqu'il n'est pas respecté. En effet, les dangers pour la protection de la vie privée des citoyens naissent davantage de l'utilisation faite de leurs données, que de la nature de celles-ci. Des informations *a priori* banales peuvent ainsi causer préjudice aux personnes concernées si elles sont utilisées dans un but illégitime[499].

> Par exemple, les dates de congé d'un fonctionnaire pourraient nuire à celui-ci si elles sont utilisées pour apprécier le droit à une promotion[500].
>
> Le registre de la DIV, contenant notamment la plaque d'immatriculation des conducteurs et leur numéro de téléphone, peut être la source de harcèlement téléphonique de jolies conductrices dont le numéro de plaque aurait été noté par un policier ayant accès à ce registre.
>
> Un fonctionnaire communal organisé et prévoyant pourrait utiliser la date de naissance des citoyens, enregistrée au Registre national, pour contacter ceux-ci le jour de leurs 70 ans afin de leur demander s'ils souhaitent réserver une concession de sépulture dans la commune.

---

protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau, Université de Montréal et Université Panthéon – Assas Paris II, septembre 2011, pp. 14 à 19.

[497] CPVP, avis n° 11/2007 du 31 mars 2007 relatif à un avant-projet de loi réglant l'application automatique des prix maximaux pour la fourniture d'électricité et de gaz naturel aux clients protégés résidentiels à revenus modestes ou à situation précaire, p. 3, n° 7.

[498] CPVP, avis n° 14/2006 du 24 mai 2006 relatif au projet d'arrêté royal déterminant les règles suivant lesquelles certaines données hospitalières doivent être communiquées au Ministre qui a la Santé publique dans ses attributions, p. 6, n° 27.

[499] Rapport fait au nom de la Commission de la Justice par Mme Mercks-Van Goey concernant le projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la proposition de loi relative à la protection de données personnelles concernant les personnes physiques dans les fichiers informatiques ou banques de données et à la création d'une commission nationale de l'informatique et des libertés, *Doc. Parl.,* Ch. Repr., sess. extr. 1991-1992, n° 413/12, p. 87 ; H. Burkert, « The dimensions of information law », *in La télématique,* T. I, Gand, Story-Scientia, 1984, p. 217 ; Y. Poullet, « L'informatique menace-t-elle nos libertés ? », *op. cit.,* p. 195 ; M.-H. Boulanger, C. de Terwangne et T. Léonard, « La protection de la vie privée à l'égard des traitements de données à caractère personnel – La loi du 8 décembre 1992 », *J.T.,* 1993, p. 377 ; B. Docquir, « Le droit de la vie privée : aperçu général et règle de proportionnalité », *in Actualités du droit de la vie privée,* (dir. B. Docquir et A. Puttemans), Bruxelles, Bruylant, 2008, pp. 32-33.

[500] CPVP, avis n° 06/97 du 19 février 1997 sur l'utilisation de données concernant les jours de maladie et évaluation de données relatives à la santé dans le cadre d'une procédure de promotion au sein du Ministère des Finances.

Ces situations malencontreuses illustrent l'importance du travail du législateur à qui il revient d'identifier, le plus minutieusement possible, le but poursuivi par chaque collecte de données effectuée par une administration et de consacrer cette finalité dans la loi, de manière à cadenasser l'utilisation de telles informations. C'est d'autant plus important que, rappelons-le, les citoyens sont contraints de fournir leurs données aux administrations.

115.- Un renforcement du pouvoir du législateur. L'exigence de finalité impose au législateur de déterminer l'objectif du traitement d'une manière assez précise. Il ne peut se contenter d'affirmer, par exemple, que le traitement de données doit correspondre aux missions de l'administration. Des indications plus fines doivent être fixées. Nous y reviendrons.

On peut d'ores et déjà affirmer que, grâce à l'exigence de finalité requise par le régime juridique de la protection des données, le législateur est en mesure de baliser, de manière assez serrée, l'action de l'administration. C'est pourquoi, face au déclin de la loi souligné dans le premier chapitre, les règles de protection des données constituent une voie intéressante pour permettre au législateur de baliser l'action de l'administration.

I. Une finalité légitime

116.- La légitimité de l'ingérence. L'article 8, §2, de la Convention européenne des droits de l'homme prévoit que l'ingérence d'une autorité publique dans le droit à la protection de la vie privée doit constituer « une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

La directive 95/46 donne écho à ces valeurs, en affirmant que « les systèmes de traitement de données sont au service de l'homme ; ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus »[501].

[501] Considérant n° 3 de la directive 95/46 précitée.

En admettant des dérogations au droit au respect de la vie privée, ces dispositions rappellent que le fonctionnement d'un État ne peut se passer de certaines ingérences dans ce droit fondamental lorsqu'elles sont motivées par le souci de satisfaire des objectifs légitimes dans une démocratie.

> Ainsi, par exemple, la bonne gestion des fonds publics impose de s'assurer que seules les personnes qui y ont droit bénéficient de tel service ou reçoivent telle allocation tout comme il importe d'instaurer des mesures de contrôles visant à endiguer la fraude fiscale, notamment.

Comme l'affirme Pierre Trudel, « invoquer le droit à la vie privée à l'encontre des mesures raisonnables de contrôle et de gestion revient à placer celui-ci au-dessus des exigences élémentaires de l'État de droit »[502]. Cela ne signifie pas pour autant qu'un objectif légitime justifie n'importe quel traitement[503].

> Par exemple, la CPVP a considéré que le contrôle et la maîtrise des dépenses d'assurance maladie en matière de soins de santé est « une finalité légitime justifiant la transmission par les organismes et établissements dispensant des [...] prestations remboursables par l'assurance maladie à des assurés sociaux ou à leurs ayants droit » car une telle finalité vise à protéger « le bien être économique du pays »[504].

Les valeurs affirmées par la Convention européenne des droits de l'homme, dans la lignée desquelles s'inscrit la directive 95/46, sont amples, et interprétées largement par la Cour européenne des droits de l'homme[505]. Celle-ci n'a d'ailleurs « jamais censuré une mesure étatique restrictive de liberté au motif que celle-ci ne poursuivrait pas l'un des buts

---

[502] P. Trudel, « Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau », mars 2003. Document disponible sur le site du Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information du Québec, http://www.institutions-democratiques.gouv.qc.ca/acces-information/documents/Rapport_Me_Pierre_Trudel.pdf

[503] Voy. *infra,* n° 117.-

[504] CPVP, avis n° 12/2002 du 21 mars 2002 relatif à un projet d'arrêté royal fixant les règles suivant lesquelles certaines données statistiques minimales psychiatriques doivent être communiquées au Ministre qui a la Santé publique dans ses attributions, p. 5, n° 11. Dans le même sens, voy. l'avis n° 10/2008, du 27 février 2008, concernant une proposition de loi relative aux certificats de bonnes conduite, vie et mœurs, p. 6, n° 28.

[505] V. Coussirat-Coustere, « Article 8 §1 », *in La Convention européenne des droits de l'homme. Commentaire article par article* (dir. L.E. Pettiti, E. Decaux et P.-H. Imbert), Paris, Economica, 1999, 2e éd., p. 336 ; B. Docquir, « Le droit de la vie privée : aperçu général et règle de proportionnalité », *op. cit.,* p. 26.

légitimes énumérés » à l'article 8, §2[506]. Il y a donc peu de chance qu'un traitement de données soit invalidé au motif qu'il viole une de ces valeurs.

C'est la raison pour laquelle la finalité d'un traitement ne peut se réduire à son assimilation à une valeur défendue par la Convention et qu'il importe d'en vérifier le caractère déterminé et explicite, comme l'expliquent les développements qui suivent[507].

117.- L'ambigüité de l'article 7 de la directive 95/46. L'article 7 de la directive 95/46 est consacré aux « principes relatifs à la légitimation des traitements de données ». Il est transposé, dans l'ordre juridique belge, par l'article 5 de la loi du 8 décembre 1992. Ces principes relatifs à la légitimation des traitements de données consistent en six hypothèses dans lesquelles un traitement peut être effectué au motif qu'il poursuit un but légitime.

> **L'article 7 de la directive 95/46** dispose que « les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :
>
> a) la personne concernée a indubitablement donné son consentement
>
> ou
>
> b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci
>
> ou
>
> c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis
>
> ou
>
> d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée
>
> ou
>
> e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées
>
> ou
>
> f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et

[506] Rapport de H. Claes et J.-J. Viseur fait au nom du groupe de travail chargé de l'examen du Titre II de la Constitution sur les clauses transversales en matière de droits et de libertés (experts : J. Velaers et S. Van Drooghenbroeck), *Doc. Parl.,* Ch. Repr., sess. 2004-2005, n° 81 2304/001, pp. 21-22.

[507] Voy. *infra,* n°s 118.- et s. et n°s 122.- et s.

libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1 ».

L'article 5 de la loi du 8 décembre 1992 reprend ces hypothèses et dispose que « le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants :

a) lorsque la personne concernée a indubitablement donné son consentement ;

b) lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

c) lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance ;

d) lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;

e) lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;

f) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi.

Le Roi peut, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, préciser les cas où la condition mentionnée sous f) est considérée ne pas être remplie ».

Ces « principes de légitimation » donnent à penser que le respect d'une de ces six hypothèses suffit pour légitimer le traitement. Dans cette interprétation, une administration pourrait penser, par exemple, qu'en obtenant le consentement des personnes concernées, elle peut commercialiser leurs données.

Agissant ainsi, l'administration en question commettrait une erreur. En effet, dans l'e-gouvernement, on ne peut pas oublier les exigences du droit administratif, et en particulier l'exigence de finalité et le principe de spécialité dont il est question ci-après[508]. Or, en cumulant les règles de protection des données et les règles de droit administratif, on constate que l'administration ne peut pas choisir entre ces six cas de légitimation. L'un d'eux doit toujours être respecté, à savoir, l'article 7, e) de la directive 95/46, repris dans l'article 5, e) de la loi du 8 décembre 1992.

[508] Voy. *infra,* nos 118.- et s.

En d'autres termes, l'administration doit toujours s'assurer que le traitement qu'elle effectue est « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique » dont elle est investie. Si cette condition n'était pas respectée, l'administration agirait en dehors des compétences qui lui ont été dévolues et commettrait donc un excès de pouvoir[509].

II. Une finalité déterminée

118.- Finalité et principe de spécialité. L'article 8, §2, de la Convention européenne des droits de l'homme exige que l'ingérence dans le droit à la vie privée soit prévue par une loi. Selon la Cour européenne des droits de l'homme, cette loi doit être rédigée de manière telle que tout individu « doit pouvoir en prévoir les conséquences pour lui »[510], ce qui suppose notamment que la loi mentionne « en quelles circonstances [...] elle habilite la puissance publique »[511] à s'ingérer dans la vie privée des intéressés.

Comme on l'a souligné dans le premier chapitre, les hautes juridictions belges abondent dans le même sens lorsqu'elles affirment que la loi requise par l'article 22 de la Constitution doit satisfaire à l'exigence de prévisibilité en déterminant, notamment, la finalité du traitement[512].

Les normes organisant la protection des données à caractère personnel traduisent cet impératif par l'obligation que tout traitement poursuive une finalité déterminée[513]. Cette exigence n'est pas inconnue du législateur ni de l'administration. En effet, traditionnellement, en droit administratif, les administrations sont tenues au respect du principe de spécialité. Celui-ci veut que les institutions n'accomplissent que les missions qui

[509] Voy. *infra* n° 120.-

[510] CEDH, arrêt *Leander c. Suède*, *op. cit.*, § 50.

[511] *Ibid.*, §51 ; CEDH, arrêt *Rotaru c. Roumanie*, *op. cit.*, § 57.

[512] C.C., arrêt n° 202/2004, *op. cit.*, B.4.5 ; C.C., arrêt n° 151/2006, du 18 octobre 2006, B. 6.1 ; C.C., arrêt n° 15/2008, *op. cit.*, B. 22 ; C.C., arrêt n° 29/2010, *op. cit.*, B.11 et s. ; C.C., arrêt n° 1/2011, *op. cit.*, B.12.1 et s. ; avis L. 41.662/1/2/3/4 des 14, 16 et 17 novembre 2006 sur un avant-projet de loi-programme (I), *op. cit.*, p. 425 ; avis L. 38.782/2/V du 11 août 2005 sur un avant-projet de loi relative à l'analyse de la menace, *op. cit.*, p. 64.

[513] L'article 8 de la Charte prévoit que les données doivent être traitées « à des fins déterminées » ; l'article 5 de la Convention n° 108 dispose que « les données à caractère personnel faisant l'objet d'un traitement automatisé sont b) enregistrées pour des finalités déterminées » tout comme l'art. 6, b), de la directive 95/46 et l'art. 4, 2°, de la loi du 8 décembre 1992.

leur ont été légalement dévolues. En outre, elles doivent le faire dans un but d'intérêt général[514].

L'exigence de finalité issue du droit de la protection des données à caractère personnel confirme le principe de spécialité consacré en droit administratif. Plus encore, il le renforce[515]. Des exemples, issus principalement de la jurisprudence de la CPVP, aident à cerner concrètement la portée de cette exigence.

A. L'exigence de finalité confirme le principe de spécialité

119.- Finalité et respect des compétences légales. La finalité d'un traitement confié à une administration doit faire partie des missions qui lui ont été légalement dévolues[516]. Cet impératif fut d'ailleurs affirmé dès les discussions préparatoires de la loi du 8 décembre 1992[517].

En outre, au sein de l'administration, seuls les fonctionnaires ayant la finalité du traitement dans leurs compétences sont habilités à traiter les

---

[514] P. Wigny, *Droit administratif,* Bruxelles, Bruylant, 1962, p. 48 ; A. Buttgenbach, *Manuel de droit administratif,* Bruxelles, Larcier, 1966, p. 49 ; A. Mast, *Précis de droit administratif belge,* Bruxelles-Gand, Story-Scientia, 1966, p. 29 ; M.-A. Flamme, *Droit administratif,* Bruxelles, Bruylant, 1989, p. 485 ; A. Mast, J. Dujardin, M. Van Damme et J. Vande Lanotte, *op. cit.,* p. 81 ; M. Nihoul, *Les privilèges du préalable et de l'exécution d'office,* Brugge, La Charte, 2001, pp. 706 à 708 ; P. Quertainmont, *Droit public économique. Interventionisme économique et avenir,* T. I, Waterloo, Kluwer, 2007, n° 66.

[515] E. Degrave et Y. Poullet, « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée », *op. cit.*, pp. 279 et 280 ; E. Degrave, « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée », *op. cit.,* p. 48.

[516] S. Gutwirth, « De toepassing van het finaliteitsbeginsel », *T.P.R.,* 1993, II, p. 1442 ; J. Dumortier, « De verplichtingen van de houder van het bestand », *in Persoonsgegevens en privacybescherming* (dir. J. Dumortier et F. Robben), Brugge, die Keure, 1995, pp. 71 et 72 ; S. Gutwirth, *Privacy and the Information Age, op. cit.,* p. 99 ; CPVP, avis n° 02/1999 du 11 janvier 1999 relatif à la diffusion de données en ce qui concerne les permis de bâtir, p. 5, n° 14 ; CPVP, avis n° 32/2001 du 10 septembre 2001 relatif à la publicité cadastrale, p. 3 ; CPVP, avis n° 07/2002 du 11 février 2002 relatif à un projet de loi créant la Banque-Carrefour des Entreprises, p. 8, n° 15 ; CPVP, avis n° 40/2006 du 27 septembre 2006 relatif à la tenue des Registres communaux de parcelles non-bâties dont question à l'article 62 du Décret flamand du 18 mai 1999 portant organisation de l'aménagement du territoire et organisation de leur publicité par internet via le futur geoloket, p. 3, n° 7 ; CPVP, avis n° 38/2008 du 26 novembre 2008 relatif à une demande d'avis du Comité sectoriel du Registre national sur le rôle du Fedict pour le compte de la Loterie Nationale, p. 4, n° 11.

[517] « Il est proposé que dans le secteur public, les traitements ne puissent avoir lieu que pour l'accomplissement des missions définies par ou en vertu d'une décision du législatif, peu importe le niveau de celui-ci ». Voy. Rapport fait au nom de la Commission de la Justice par Mme Mercks-Van Goey concernant le projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la proposition de loi relative à

données collectées à cette fin. On considère qu'ils ont un « intérêt fonctionnel »[518] à prendre connaissance des données traitées.

> Un avant-projet de loi organisant la collecte d'informations par le SPF Finances en vue de l'établissement et de la perception de l'impôt prévoyait que tous les agents du SPF Finances auraient accès aux données collectées à cette fin. La CPVP s'est prononcée défavorablement face à cette solution. Elle a soutenu, à juste titre, que « seuls les fonctionnaires des administrations fiscales et du SPF Finances régulièrement chargés de l'établissement, de la perception et du recouvrement de l'impôt sont légitimement habilités à traiter des informations, et plus spécifiquement des données à caractère personnel, dans le but d'assurer l'établissement, la perception et le recouvrement de l'impôt. À défaut, si l'habilitation à traiter ces données était plus étendue, le traitement de données présenterait un défaut de loyauté et de licéité (non respect de l'article 4, §1er, 1° de la [loi du 8 décembre 1992]). Il excéderait les compétences et pouvoirs de ceux qui le réaliseraient et ne s'avérerait donc pas nécessaire à l'exercice de leur mission (non respect de l'article 5, al. 1, e) de la [loi du 8 décembre 1992]). Tous les agents du SPF Finances ne peuvent donc plus être autorisés à traiter l'ensemble des renseignements en possession de l'administration. Chaque fonctionnaire qui prend connaissance de données à caractère personnel doit toujours avoir un intérêt fonctionnel concret à pouvoir prendre connaissance de ces données »[519].
>
> Pour illustrer cet avis de la CPVP, prenons l'exemple d'un fonctionnaire de l'administration fiscale chargé d'appliquer les droits d'enregistrement à la vente d'un immeuble. Pour calculer l'exact montant de ces droits, il aura besoin de connaître le montant du revenu cadastral de l'immeuble, donnée collectée par ses collègues chargés de la perception de l'impôt sur le revenu. Il pourra certainement obtenir la communication de la donnée relative au montant du revenu cadastral de l'immeuble mais il ne pourrait en aucun cas accéder à des données collectées par ses collègues et qui n'ont pas de lien avec le calcul des droits d'enregistrement. Tel serait le cas s'il pouvait accéder à des renseignements relatifs aux charges de famille du contribuable ou à l'existence d'un handicap qui justifie des réductions d'impôts, etc.[520].

Cet avis de la CPVP mérite d'être salué en ce qu'il met en évidence le fait qu'on ne peut, à l'occasion d'un traitement de données à caractère personnel, conférer à une administration et à ses agents, des compétences

---

la protection de données personnelles concernant les personnes physiques dans les fichiers informatiques ou banques de données et à la création d'une commission nationale de l'informatique et des libertés, *op. cit.*, p. 87

[518] CPVP, avis n° 29/2009, *op. cit.*, p. 3, § 7.

[519] *Idem.*

[520] Cet exemple est expliqué par P. Glineur, « La fiscalité et l'informatique… vers la naissance d'une droit fiscal de l'informatique », *R.G.F.*, 1984, p. 80.

qu'ils n'ont pas[521]. En effet, l'informatique demeure un outil, « une aide à l'exécution des tâches publiques »[522]. La finalité poursuivie par cet outil doit rester cantonnée aux missions que la loi confie à l'administration et à ses agents. En d'autres termes, le principe de spécialité doit englober l'exigence de finalité.

B. L'exigence de finalité renforce le principe de spécialité

120.- Une exigence de précision. L'exigence de finalité ne se satisfait pas du respect du principe de spécialité. Elle le renforce. En effet, l'exigence de détermination de la finalité s'assimile à une exigence de précision de celle-ci. Comme l'affirme la CPVP, plus la finalité est définie précisément, plus on refreine les usages abusifs de données à caractère personnel[523].

De manière plus générale, l'exigence de finalité permet également de lutter contre l'excès de pouvoir dont l'administration pourrait se rendre coupable. On vise le fait d'agir dans un but d'intérêt général qui diffère de celui que le législateur avait en vue en confiant la mission de service public.

Certaines autorités ont déjà été condamnées pour avoir commis un excès de pouvoir alors qu'elles agissaient dans l'intérêt général. Tel fut le cas notamment d'un bourgmestre ayant ordonné la démolition d'un immeuble menaçant de s'effondrer, à des fins archéologiques et non liées à la sécurité publique[524]. Grâce à sa précision, l'exigence de finalité empêche que l'autorité administrative doive « deviner » dans quel but d'intérêt général précis elle doit agir[525].

---

[521] Dans le même sens, P. Glineur, *op. cit.*, p. 80 qui soutenait déjà jadis que les banques de données au sein de l'administration – l'occurrence, l'administration fiscale – ne peuvent aboutir à « apporter dans les services de l'administration des informations superflues par rapport au but poursuivi, en l'espèce, la perception d'un impôt bien déterminé. Une pareille 'surinformation' [...] ne nous paraît pas licite car elle ne répond pas au principe de 'spécialité' qui guide l'action administrative (et donc également l'information administrative), principe qui veut que chaque service administratif limite son activité à ce qui constitue l'objet de la mission qui lui a été confiée ».

[522] H. Burkert, « Le jugement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses conséquences », *D.I.T.,* 1985, p. 9.

[523] Voy. not. CPVP, avis n° 06/2006 du 1er mars 2006 concernant l'avant-projet de décret du Parlement de la Région wallonne relatif au recueil de données épidémiologiques sur les malformations congénitales, p. 6, n° 28. Dans le même sens, CPVP, avis n° 30/2006 du 26 juillet 2006 relatif à une demande d'avis concernant un projet d'arrêté royal modifiant l'arrêté royal du 19 mars 2004 réglementant le traitement de substitution, p. 6, n° 24.

[524] Liège, 24 novembre 1969, *J.A.L.,* 1969-1970, p. 289.

[525] E. Degrave et Y. Poullet, « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée », *op. cit.*, p. 280

Concrètement, les avis de la CPVP privée livrent des indices aidant le législateur à atteindre la précision requise lors de la définition d'une finalité.

a) Exclusion des critères imprécis. Tout d'abord, le législateur ne peut se contenter de prévoir que la finalité doit entrer *dans les missions* de l'administration concernée.

> Par exemple, une source authentique de données ne peut être créée dans le seul but de permettre « l'exécution de diverses 'tâches de service public' »[526] des administrations ou l'accomplissement de la « mission générale du service de gestion »[527] de cette banque de données. Prévoir qu'une administration a accès au Registre national « pour l'exécution de ses missions d'intérêt général » est également une formulation trop imprécise[528].
>
> C'est pourquoi, selon nous, est contraire à cet impératif la disposition légale en vigueur selon laquelle « le Service public fédéral Finances collecte et traite des données à caractère personnel afin d'exécuter ses missions légales. Les données ne peuvent être utilisées par le Service public fédéral Finances à d'autres fins que l'exécution de ses missions légales »[529].

Dans le même sens, une finalité ne peut être définie à ce point largement qu'elle permette *tous les traitements* effectués par l'instance concernée.

> Ainsi, « la communication interne et externe requise par le fonctionnement de la justice » n'est pas une finalité suffisamment précise pour permettre le traitement de données à caractère personnel au sein du système

[526] CPVP, avis n° 42/2006 du 18 octobre 2006 concernant l'avant-projet de loi portant création d'une source authentique des données relatives aux véhicules, p. 6, n° 19.

[527] CPVP, avis n° 23/2008 du 11 juin 2008 relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules, p. 20, n° 57.

[528] CPVP, avis n° 19/2002 du 10 juin 2002 concernant le projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, p. 7, n° 11. Dans le même sens, à propos de l'utilisation de la notion de « tâches liées à la gestion administrative » pour définir une finalité, voy. CPVP, avis n° 29/95 du 27 octobre 1995 relatif au projet d'arrêté royal autorisant l'accès au fonds national de la Recherche scientifique aux informations du Registre national des personnes physiques, p. 4, n° 6 ; l'avis n° 10/96 du 15 mai 1996 relatif au projet d'arrêté royal autorisant le Fonds du Logement des Familles nombreuses de Wallonie, à accéder au Registre national des personnes physiques et à en utiliser le numéro d'identification, p. 4 et l'avis n° 11/96 du 15 mai 1996 relatif au projet d'arrêté royal autorisant la Société Régionale Wallonne du Logement et les sociétés immobilières de service public agréées par celle-ci à accéder au Registre national des personnes physiques et à en utiliser le numéro d'identification, p. 6.

[529] Art. 3 de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions, *M.B.*, 24 août 2012.

d'information « Phénix ». En effet, selon la CPVP, « cette mention est peu spécifique et couvre toutes les applications tant d'une administration que d'une entreprise »[530].

Dans le même sens, la CPVP s'est prononcée sur l'enregistrement, par les hôpitaux, du résumé hospitalier minimum et des données « service mobile d'urgence », destinés à être transmis au Ministre de la Santé publique. Elle a estimé que les finalités décrites n'étaient pas suffisamment précises puisqu'elles légitiment « le traitement de quasiment toutes les données enregistrées dans un hôpital »[531].

b) Fin en soi. En outre, la CPVP a soutenu que la finalité doit constituer une fin en soi, et non simplement un moyen d'atteindre cette fin[532].

On peut raisonnablement supposer que cette exigence s'explique du fait qu'un même moyen pourrait servir diverses finalités, qui n'entreraient pas toutes nécessairement dans les compétences légalement définies du responsable du traitement.

---

[530] CPVP, avis n° 11/2004 du 4 octobre 2004 relatif à deux avant-projets de loi instituant la banque de données-Phénix, n° 8 et n° 10.

[531] CPVP, avis n° 14/2006 du 24 mai 2006, *op. cit.*, n° 27. En ce qui concerne l'enregistrement du résumé hospitalier minimum, l'article 3 du projet d'arrêté royal définit la finalité du traitement comme suit : « § 1 L'enregistrement du Résumé Hospitalier Minimum a pour objectif de soutenir la politique sanitaire à mener, en ce qui concerne notamment : 1° la détermination des besoins en matière d'établissements hospitaliers ; 2° la description des normes d'agrément qualitatives et quantitatives des hôpitaux et de leurs services ; 3° l'organisation du financement des hôpitaux ; 4° la définition de la politique relative à l'exercice de l'art de guérir ; 5° la définition d'une politique épidémiologique. § 2 L'enregistrement du Résumé Hospitalier minimum a également pour objectif de soutenir la politique au sein des hôpitaux, notamment par le biais d'un feed-back général et individuel de sorte que les hôpitaux puissent se positionner et de sorte que les hôpitaux puissent corriger leur politique interne » ; En ce qui concerne l'enregistrement des données dans le cadre de la fonction « service mobile d'urgence », l'article 19 du projet d'arrêté royal définit la finalité du traitement comme suit : « L'enregistrement des données SMUR vise à soutenir la politique de la santé à mener, entre autres en ce qui concerne 1° l'évaluation de la programmation des fonctions « SMUR » agréées, en particulier de sorte que la programmation soit suffisante en fonction de la répartition géographique et en fonction du nombre de « SMUR » qui sont intégrés dans le fonctionnement de l'aide médicale urgente en vertu de l'article 1er de l'arrêté ministériel du 29 janvier 2003 intégrant des fonctions « service mobile d'urgence » agréées dans le fonctionnement de l'aide médicale urgente 2° l'évaluation du fonctionnement des fonctions « SMUR », plus précisément dans le domaine d'une prise en charge adéquate et immédiate des malades ou des victimes d'accidents ».

[532] Ce raisonnement de la CPVP a été utilisé pour critiquer une décision du Comité sectoriel Registre national qui autorisait l'accès de Fedict au Registre national en vue de « tester, corriger et entretenir des applications informatiques qui ont une connexion avec le registre national via l'U.M.E., le F.S.B. et les webservices ». Voy. Y. POULLET, « Quelques réflexions à propos de la délibération n° 19/2008 du 7 mai 2008 émanant du comité sectoriel registre national », *R D.T.I.,* 2008, p. 413.

> Ainsi, on ne peut admettre l'enregistrement, par une administration, de données relatives au véhicule des individus dans le seul but d'en « connaître le kilométrage ». En effet, ce dernier élément n'est qu'un moyen de réaliser un objectif final qu'il y a lieu de déterminer, à savoir, en l'occurrence, la protection des consommateurs contre la fraude relative au kilométrage[533].
>
> Dans le même sens, on ne peut assigner comme finalité à une banque de données celle de « recueillir et centraliser les informations sur l'état de l'emploi dans le secteur public de la Région [Bruxelles-capitale] »[534]. Il y a lieu de définir le but poursuivi par ce traitement, qui ne peut être que celui d' « établir des statistiques anonymes pour soutenir la politique dans un certain nombre de domaines à préciser »[535].
>
> Cette position est également confirmée en ce qui concerne les missions de la Banque-Carrefour des Entreprises. Plutôt que de dire que cette source authentique est chargée « de la récolte, du stockage et de la gestion des données portant sur l'identification des titulaires d'une inscription », il est préférable de préciser qu'elle assure « l'enregistrement, la mémorisation et la communication d'informations permettant l'identification des entreprises et la localisation des dossiers relatives à ces entreprises dans les diverses administrations et ce afin de faciliter les relations entre administrations et administrés et la fiabilité des échanges entre administrations »[536].

c) Critère fonctionnel. Pour constituer une fin en soi, la finalité doit être décrite à l'aide d'un critère fonctionnel et non un critère organique. En d'autres termes, il ne faut pas seulement se demander à qui le traitement de données à caractère personnel doit servir (critère organique) mais bien pour quelle(s) raison(s) telle administration veut effectuer de tels traitements (critère fonctionnel).

> Ainsi, on ne peut admettre le traitement des informations « nécessaires au service des caisses locales des dépôts et consignations ». Il faut utiliser un critère fonctionnel « répondant à la question de savoir pour quelle(s) finalité(s) le service des caisses locales des dépôts et consignations réalise des traitements de données à caractère personnel »[537].

---

[533] CPVP, avis n° 15/2006 du 14 juin 2006 relatif au projet d'arrêté royal réglant la collaboration à l'association chargée de l'enregistrement du kilométrage des véhicules, n° 48.

[534] CPVP, avis n° 02/97 du 8 janvier 1997, relatif au projet d'arrêté de la Région de Bruxelles-Capitale créant une banque de données concernant le personnel du ministère de la Région de Bruxelles-Capitale et des organismes d'intérêt public qui dépendent de la région de Bruxelles-Capitale, p. 3, n° 5.

[535] *Ibid.*, p. 3, n° 5.

[536] CPVP, avis n° 07/2002 du 11 février 2002 relatif à un projet de loi créant la Banque-Carrefour des Entreprises, p. 6, n° 11.

[537] CPVP, avis n° 01/2007 du 17 janvier 2007, concernant un avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances, p. 6, n° 27.

d) Finalité de gestion administrative et finalité de contrôle. Enfin, il est recommandé de distinguer, parmi les finalités définies à partir d'un critère fonctionnel, les tâches de *gestion administrative*, d'une part, et les tâches de *contrôle*, d'autre part.

Selon nous, une telle distinction permet non seulement de perfectionner l'exigence de finalité, mais elle s'avèrera également utile si l'on souhaite, à l'avenir, réutiliser les données. Cela facilitera le nécessaire examen de compatibilité entre la finalité poursuivie lors de la collecte initiale des données et celle poursuivie lors de leur réutilisation[538].

> Par exemple, la CPVP[539] a approuvé le fait que, dans un avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances, le législateur ait indiqué que celui-ci ne peut utiliser les données à caractère personnel que dans la mesure de ce qui est nécessaire « a) aux opérations de gestion administrative pour l'établissement et la perception des impôts, taxes droits et accises ; b) aux opérations de contrôle, de recouvrement et à celles liées à la gestion du contentieux des impôts, taxes, droits et accises [...] »[540] effectuées par l'Administration générale Impôts et recouvrement.

121.- Conséquences. La détermination précise des finalités a des conséquences sur l'organisation interne de l'administration.

Selon la CPVP, à la « séparation fonctionnelle des [...] tâches, doit correspondre une séparation institutionnelle [...] Il s'agit là d'une application du principe de la distinction même des finalités »[541]. Une même personne ne peut donc pas être chargée de plusieurs traitements poursuivant des finalités distinctes. En d'autres termes, les données collectées pour des finalités différentes doivent être utilisées par des personnes différentes.

Le constat est non négligeable : au travers de l'exigence de précision de la finalité, on aboutit à une séparation des pouvoirs en matière d'information au sein de chaque autorité, qui perfectionne encore davantage le principe de spécialité des administrations. On constate alors qu'au principe de la séparation des pouvoirs s'ajoute, au sein du pouvoir exécutif, un principe de la « séparation des pouvoirs en matière d'information »[542].

---

[538] Voy. *infra*, n°s 124.- et s.

[539] CPVP, avis n° 01/2007, *op. cit.,* p. 5, n° 21.

[540] Avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service Public fédéral Finances, *Doc. Parl.,* Ch. Repr., sess. 2006-2007, n° 51 3064/001, p. 42.

[541] CPVP, avis n° 01/2007, *op. cit.,* p. 7, n° 12*bis*.

[542] H. Burkert, « Le jugement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses conséquences », *op. cit.,* p. 12.

Par exemple, certains services publics fédéraux, tels que le SPF Finances, sont composés de plusieurs départements. Chacun de ces départements peut être amené, dans le cadre de ses missions, à collecter des données nécessaires pour la gestion administrative des tâches, et d'autres, pour réaliser des opérations de contrôle des citoyens. La CPVP recommande que « les processus de gestion des dossiers au sein des multiples services des directions générales séparent clairement les personnes en charge des opérations de traitement à finalité de gestion administrative de celles en charge des opérations de traitement à finalité de contrôle »[543].

Dans le même sens, la CPVP a remarqué que le Centre fédéral d'expertise poursuivait deux finalités : d'une part, la mise en place d'un réseau de la santé et la réalisation, dans ce cadre, de l'inventaire des données présentes dans ce réseau ; d'autre part, la réalisation de rapports et d'études sur la base de ces ressources informationnelles. Elle a alors affirmé qu'il était « nécessaire de bien séparer ces deux finalités et d'en confier la responsabilité à des instances différentes, sous peine de voir le réseau et l'inventaire des ressources défini très largement par ceux-là même qui seront en charge de l'exploiter et souhaiteront pour des raisons évidentes liées à leurs besoins de recherche disposer du maximum d'informations »[544].

III. Une finalité explicite

122.- Des termes clairs. L'exigence de prévisibilité imposée par l'article 22 de la Constitution impose que la finalité déterminée par le législateur soit explicite, c'est-à-dire, reprise, textuellement, dans la norme légale qui la définit.

L'obligation d'une finalité explicite est d'ailleurs formellement consacrée par l'article 6, b), de la directive 95/46 et l'article 4, 2°, de la loi du 8 décembre 1992.

Concrètement, le législateur doit faire œuvre de pédagogie pour que la finalité soit exposée le plus clairement possible. Il ne suffit donc pas de reprendre, dans la norme, quelques exemples de finalités pouvant être poursuivies. Une liste limitative des finalités poursuivies doit figurer dans le texte[545].

---

[543] CPVP, avis n° 01/2007, *op. cit.*, p. 5, n° 22.

[544] CPVP, avis n° 33/2002, *op. cit.*, p. 7, n° 12*bis*. Voy. dans le même sens, l'avis n° 23/2008, *op. cit.*, pp. 16 et 17, n°s 43 à 45.

[545] CPVP, avis n° 42/2006, *op. cit.*, p. 7, n° 24. Sur la question de la finalité de réutilisation compatible avec la finalité de la collecte des données, voy. *infra*, n°s 124.- et s.

En outre, la CPVP estime utile de faire figurer, dans la norme organisant le traitement de données à caractère personnel, non seulement la finalité poursuivie, mais également les finalités que ne peut poursuivre l'administration concernée. *A priori,* le recours à la « définition négative » de la finalité semble judicieux lorsque, au vu des données utilisées ou de l'outil mis en place, on peut aisément craindre certains traitements qui ne respectent pas la *ratio legis* de la loi organisant le traitement. Néanmoins, bien qu'elle ait le mérite de la clarté, la technique de la « définition négative » de la finalité risque d'affaiblir la portée de la « définition positive ». Ce faisant, ne risque-t-on pas d'utiliser des données pour réaliser certaines finalités qui n'ont pas été prévues par le législateur au motif que ce dernier ne les a pas interdites ? Il semble préférable de faire figurer les finalités qui ne peuvent être poursuivies dans l'exposé des motifs et de veiller à la précision de la finalité positive, particulièrement lorsque des données susceptibles d'un usage abusif sont en cause.

123.- Précision et apaisement. Quoi qu'il en soit, les conseils donnés par la CPVP rappellent que la protection de la vie privée des citoyens, entendue comme le droit à l'autodétermination informationnelle, impose que l'exigence de prévisibilité soit interprétée d'autant plus sévèrement que le type de données ou l'outil mis en place génèrent des craintes auprès des personnes concernées. Ces dernières ont le droit d'être rassurées, à la lecture de la loi, quant à l'utilisation de leurs données.

Tel est le cas, par exemple, lorsque les données utilisées pourraient aisément être vendues au secteur privé, ou enregistrées par une plate forme d'échange alors que la loi ne le prévoit pas.

> Par exemple, les données relatives aux véhicules génèrent une méfiance particulière compte tenu du fait qu'elles ont jadis été communiquées abusivement aux concessionnaires automobiles à des fins de marketing direct[546]. Parmi celles-ci, les informations relatives au kilométrage des véhicules ont, selon la CPVP, une valeur financière importante dans le secteur privé. Elles peuvent par exemple être réutilisées par des compagnies d'assurances pour calculer des primes adaptées à la vétusté du véhicule. Des abus sont également possibles au sein du secteur public. Il serait ainsi tentant, pour l'administration fiscale, d'avoir accès à ces données pour contrôler, par exemple, les « kilomètres professionnels » figurant dans la déclaration fiscale[547]. C'est pourquoi, la CPVP recommande d' « interdire explicitement l'utilisation

[546] CPVP, avis n° 14/2010, *op. cit.,* p. 8, n° 32.
[547] CPVP, avis n° 15/2006, *op. cit.,* n° 59.

> d'informations du traitement de Car-Pass[548] [...] par des professionnel, des vendeurs ou des tiers (par ex. assureurs, sociétés de leasing) pour des finalités qui n'ont pas de fondement légal légitime »[549].

La crainte d'un enregistrement des données à caractère personnel par la plateforme *eHealth* a été invoquée devant la Cour constitutionnelle par la Ligue des droits de l'homme, lors d'un recours en annulation intenté contre la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth[550]. Selon les requérants, « la loi ne spécifie aucunement [...] que la plateforme eHealth ne viserait pas un enregistrement central de données à caractère personnel »[551]. La Cour a répondu qu'il ne ressortait pas des finalités consacrées par la loi que la plateforme était compétente pour enregistrer les données, et qu'il « revient au juge compétent de veiller au respect de cette exigence de la loi »[552].

Si l'arrêt de la Cour constitutionnelle vient certes interpréter ladite loi dans un sens favorable à la protection de la vie privée, on regrette que la finalité définie par la loi ne soit pas suffisamment précise pour éradiquer toute crainte de la part des citoyens au sujet de l'utilisation de données sensibles car elles touchent à leur état de santé et ont vocation à circuler au sein de très nombreuses institutions.

IV. Une finalité compatible

124.- La condition de réutilisation des données. Les normes protectrices des données à caractère personnel affirment que les données ne peuvent pas être « traitées ultérieurement de manière incompatible »[553] avec la finalité de leur collecte. Si aucune limite n'était fixée pour réutiliser des données, chaque administration serait en mesure de connaître chaque

---

[548] Nous signalons que le « Car-Pass » est le document fourni lors de l'achat d'un véhicule d'occasion et qui mentionne notamment le kilométrage du véhicule à différentes dates. Au sujet du traitement de données qu'il implique, voy. E. Degrave et Y. Poullet, « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée », précité.

[549] CPVP, avis n° 15/2006, *op. cit.*, n° 65.

[550] C.C., arrêt n° 29/2010, précité.

[551] *Ibid.*, A. 3.3.

[552] *Ibid.*, B.13.1.

[553] Art. 6, b) de la directive 95/46 ; art. 4, §1er, 2° de la loi du 8 décembre 1992. La Convention n° 108 prévoit une exigence similaire en soutenant, en son art. 5, b), que « les données à caractère personnel faisant l'objet d'un traitement automatisé [...] ne sont pas utilisées de manière incompatible avec » les finalités de la collecte. La Charte des droits fondamentaux ne spécifie rien quant à la réutilisation des informations.

information personnelle de chaque personne. Dans un tel contexte, les citoyens ne pourraient pas contrôler l'usage qui est fait de leurs données et l'autodétermination informationnelle serait un leurre.

> En ce sens, la Commission d'accès à l'information du Québec s'inquiète de « la tendance marquée vers la concentration et la centralisation de plus en plus grandes de renseignements personnels dans tous les secteurs d'activité de l'appareil gouvernemental » et insiste sur l'importance de la finalité pour garantir l' « étanchéité des fichiers ». Elle rappelle que « sans étanchéité des fichiers de renseignements personnels, les organismes publics ne seront plus en mesure de garantir aux citoyens qu'ils respectent leur droit de savoir à quelles fins sont utilisés les renseignements personnels »[554].

La loi du 8 décembre 1992 précise que la compatibilité doit être appréciée « compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables »[555]. Cette exigence de compatibilité s'impose lorsqu'une administration souhaite utiliser des données déjà collectées par une autre administration, afin de ne pas devoir les demander une nouvelle fois à la personne concernée. Une telle réutilisation n'est possible qu'à la condition que la finalité de la réutilisation – souvent appelée « finalité ultérieure » ou « finalité secondaire » soit compatible avec la finalité de la collecte initiale des données.

> Entre autres exemples, la CPVP considère que les données du registre de la Direction de l'Immatriculation des véhicules peuvent être réutilisées par les services d'incendie en vue d'identifier les propriétaires des véhicules qui sont redevables d'une indemnité suite à une intervention des sapeurs pompiers[556].
>
> À l'inverse, un Bourgmestre ne peut réutiliser les données du registre de la population pour envoyer, en son nom personnel, une carte de félicitations aux jubilés de sa commune. Une telle réutilisation des données poursuivrait un objectif de propagande électorale, ce qui n'est pas compatible avec la

[554] Commission d'accès à l'information du Québec, Une réforme de l'accès à l'information : le choix de la transparence. Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé, Novembre 2002, p. 101, disponible à l'adresse www.cai.gouv.qc.ca

[555] Art. 4, §1er, 2°, de la loi du 8 décembre 1992.

[556] CSAF, délibération n° 22/2012 du 22 septembre 2012 relative à une demande 'autorisation formulée par les services d'incendie et par la protection civile afin de pouvoir consulter certaines données enregistrées auprès de la Direction pour l'immatriculation des véhicules du SPF Mobilité et Transports (AF-MA-2012-034).

finalité initiale du registre de la population, conçu pour satisfaire aux missions administratives de certaines autorités déterminées[557].

125.- De nombreuses questions. Compte tenu du principe de la collecte unique et de la volonté d'encourager la circulation des données entre les administrations qui fondent l'e-gouvernement belge, l'exigence de compatibilité revêt une importance cardinale.

Et pourtant… les choses sont, ici encore, loin d'être claires. L'appréciation de la compatibilité se heurte à bien des questions. Qu'entendre concrètement par « prévisions raisonnables de l'intéressé » ? Les « dispositions légales et réglementaires » imposent-elles l'existence d'une base légale et/ou réglementaire ? Doivent-elles viser l'administration qui livre la donnée et celle qui la reçoit, ou l'une d'entre elles seulement ? Les « dispositions légales et réglementaires » et les « prévisions raisonnables de l'intéressé » sont-elles des conditions cumulatives, ou non ?

Nombre d'hésitations liées à ces questions traversent les avis de la CPVP, créant une jurisprudence malheureusement peu constante[558]. Il s'impose dès lors de confronter ces notions au regard du droit administratif et tenter de résoudre ensuite les difficultés qu'elles génèrent.

126.- Une difficulté transfrontalière. Remarquons que, d'après nos recherches, aucun État ne semble détenir de « solution miracle » pour apprécier la compatibilité de finalités.

L'exigence de compatibilité, consacrée par la directive 95/46, est transposée de manière identique ou très semblable dans la plupart des États-membres. Néanmoins, chaque État est confronté au problème de l'application de cette exigence vague. Les lois nationales prévoient des critères différents pour tenter d'apprécier la compatibilité en pratique, mais celle-ci demeure périlleuse quel que soit le pays concerné[559].

---

[557] C'est pourquoi, la CPVP recommande que ce type d'envoi se fasse à l'initiative de la commune, et non d'une personne isolée. Voy. CPVP, recommandation n° 06/2012 du 2 mai 2012 relative à la communication d'informations contenues dans les registres de la population en application de l'arrêté royal du 16 juillet 1992 relatif à la communication des informations contenues dans les registres de la population et dans le registre des étrangers.

[558] Voy. E. Degrave, « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée », *op. cit.*, pp. 67-70.

[559] Sur ces aspects de droit comparé, et pour de plus amples détails sur l'application de la directive 95/46/CE dans les législations nationales, voy. les analyses de D. Korff, parmi lesquelles *Data Protection Laws in the European Union,* Bruxelles, Federation of European Direct and Interactive Marketing, 2005 ; « Comparative summary of national laws », *EC Study of implementation of data protection directive*, septembre 2002 ; « Data protection laws

En *Allemagne* par exemple, on recourt à un « test d'équilibre » qui consiste principalement à analyser si le destinataire des données dispose d'un intérêt légitime qui prévaut sur l'intérêt des personnes concernées à ce que leurs données ne soient pas réutilisées. Cet intérêt légitime doit être manifeste[560].

Aux *Pays-Bas*, l'examen de compatibilité est également effectué à partir de certains tests d'équilibre. La loi prévoit un certain nombre de critères pour juger de la compatibilité entre la finalité primaire et secondaire. Ainsi y a-t-il lieu d'être attentif à la relation entre les deux finalités, à la nature des données, aux conséquences de la réutilisation pour la personne concernée, aux garanties offertes à cette dernière, etc.[561]

En *Irlande*, on impose l'existence d'un lien étroit entre les deux finalités tout en recourant, comme en Belgique, au critère des « prévisions raisonnables »[562].

En *Fran*ce, on ne recourt pas à un critère en particulier. L'examen est réalisé au cas par cas, principalement au regard des dispositions légales qui obligent le citoyen à donner ses informations[563].

Les choses ne semblent pas être plus simples en dehors de l'Union européenne.

Le *Canada*, par exemple, est lui aussi confronté à des préoccupations semblables, appliquant le critère de compatibilité aux échanges de données dans l'administration[564]. Le paragraphe 8 (2) de la loi sur la protection des renseignements personnels établit une liste de 12 cas d'autorisation, critiqués pour leur caractère trop laxiste. Ces critiques s'adressent en particulier au point m) qui prévoit la licéité de la communication lorsque « des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée ». Cela fait donc plusieurs années que le Commissariat à

in EU : the difficulties in meeting the challenges posed by the global social and technical developments », 20 janvier 2010, European Commission DJ Justice, Freedom and Security report, disponible sur le site http://ssrn.com/abstract=1638949.

[560] Bundesdatenschutzgesetz, Section 14 (2)

[561] Wet gemeentelijke basisadministratie persoonsgegevens, Art. 9 (2).

[562] *Data protection Act*, Section 2 (c).

[563] Art. 6, 2°, de la loi informatique et libertés. Pour des exemples de cas examinés, voy. le site internet de la CNIL et not., http://www.cnil.fr/la-cnil/actu-cnil/article/article/une-mairie-condamnee-pour-utilisation-detournee-des-donnees-du-recensement/

[564] Art. 7 de la loi canadienne sur la protection des renseignements personnels disponible sur le site http://laws.justice.gc.ca/PDF/Readability/p-8.6.pdf. À ce sujet, voy. R. Duaso Cales, *op. cit.,* pp. 172 à 193.

la protection de la vie privée du Canada, notamment, réclame une modification de la loi[565].

Selon le Commissariat à la protection de la vie privée du Canada, « la notion d'usage compatible' est sans doute l'une des notions les plus problématiques de la loi. Malgré le fait que ce problème ait été relevé il y a près de vingt ans, lors de l'examen de 1987, aucune amélioration n'a été apportée à cet égard [...] Dans l'éventualité où la notion 'd'usage compatible' serait conservée dans la *Loi sur la protection des renseignements personnels,* elle devra être définie de manière claire et limitée. L' 'usage compatible' dans le cadre du mandat général d'une institution gouvernementale ne constitue pas une justification suffisante, et en aucun cas, on ne peut faire appel au couplage de données sous prétexte qu'il constitue un usage compatible »[566].

Quoi qu'il en soit, aucun État ne semble détenir un critère infaillible permettant d'éviter toute discussion. L'appréciation de la compatibilité reste parée d'une certaine dose de subjectivité et conduit presque nécessairement à une appréciation au cas par cas.

> En 2007 déjà, le contrôleur européen de la protection des données a demandé à la Commission de « recourir à une communication interprétative » concernant notamment le concept « d'utilisations incompatibles »[567]. À notre connaissance, cela n'a malheureusement pas encore été fait.

A. Les « dispositions légales et réglementaires » et les « prévisions raisonnables de l'intéressé »

127.- Des critères critiquables. À y regarder d'un peu plus près, les deux critères qu'utilise la loi du 8 décembre 1992 pour préciser la notion de « compatibilité » n'apportent rien de neuf par rapport à ce que l'on pouvait déjà déduire du droit administratif. Il ne s'agit donc pas d'impératifs propres à la protection des données.

128.- Des notions superflues. Les « dispositions légales et réglementaires applicables » constituent une application de l'exigence de légalité

---

[565] Voy. not. Commissariat à la protection de la vie privée du Canada, *Réforme de la Loi sur la protection des renseignements personnels,* Juin 2006, disponible sur le site http://www.priv.gc.ca

[566] *Idem.*

[567] Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, *J.O.C.E.,* C. 255, 27 octobre 2007, pp. 1-12.

et du principe de spécialité traditionnellement applicables aux administrations. Ces dernières ne peuvent agir que dans le cadre des compétences légales qui leur ont été attribuées. Ce souci est d'ailleurs déjà rencontré par l'exigence d'une finalité « déterminée »[568].

Par ailleurs, le recours au « prévisions raisonnables de l'intéressé » renvoie à l'exigence de prévisibilité que l'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution imposent à toute ingérence dans le droit à la vie privée. On ne peut tirer de la loi des conséquences que le citoyen n'a pas pu prévoir. Ce souci est lui aussi déjà rencontré par l'exigence d'une finalité « déterminée » et « explicite »[569].

129.- Des notions floues. Les critères de compatibilité sont flous et soulèvent plusieurs questions.

a) Des conditions cumulatives ? Tout d'abord, les « dispositions légales et réglementaires » et les « prévisions raisonnables des intéressés » sont-elles des conditions cumulatives ou non ?

Prônant le cumul de ces conditions, la CPVP a affirmé à plusieurs reprises que « le fait que le législateur autorise explicitement un traitement ultérieur pour une certaine finalité ne le légitime pas ipso facto à la lumière de l'article 4 de la [loi du 8 décembre 1992] »[570]. Néanmoins, dans certains avis, elle adopte la position contraire, en considérant que le respect d'un de ces critères seulement suffit à satisfaire l'exigence de compatibilité[571].

Pourtant, étant donné que la légalité, la spécialité et la prévisibilité doivent toutes trois être distinctement respectées par les administrations, les « dispositions légales et réglementaires applicables » et les « prévisions raisonnables de l'intéressé » doivent, à notre sens, être imposées cumulativement.

---

[568] Voy. *supra,* n° 120.-

[569] Voy. *supra*, n° 122.-

[570] Voy. not., l'avis n° 17/2005 du 9 novembre 2005 relatif à l'avant-projet de loi modifiant l'article 5 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, p. 4, n° 6.4. et l'avis n° 49/2006, *op. cit.,* p. 4, n° 25.

[571] CPVP, avis n° 30/96 du 13 novembre 1996 relatif à un avant-projet de loi adaptant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel à la Directive 95/45/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, p. 7, n° 10 ; avis n° 18/2008 du 30 avril 2008 demandé par la Région de Bruxelles-Capitale, Administration de l'Aménagement du Territoire et du Logement, Direction de l'Inspection régionale du Logement relatif à la communication à une administration communale de données recueillies en application du Code bruxellois du Logement, pp. 5 à 8.

b) Base légale ou base réglementaire ? La question se pose aussi de savoir si une base légale ou une base réglementaire est requise pour organiser une réutilisation de données. Par ailleurs, un tel fondement normatif est-il exigé dans le chef de l'administration émettrice et/ou destinatrice des données ?

b-1. Les avis de la CPVP n'offrent pas une réponse claire quant à savoir si la loi du 8 décembre 1992 exige une base légale ou réglementaire à la base d'une réutilisation de données. Elle semble considérer que le choix d'une base légale ou d'une base réglementaire dépend des prévisions raisonnables des intéressés.

Ainsi, si les personnes concernées ont pu raisonnablement prévoir la réutilisation des données envisagées, la CPVP estime que la réutilisation de données est effectuée « à titre complémentaire »[572] de leur collecte. C'est pourquoi, une base réglementaire suffit.

> Par exemple, la communication des données détenues par la Direction générale de l'agriculture (DGA) à la Direction générale des Ressources naturelles et de l'Environnement (DGRNE) peut être fondée sur un arrêté compte tenu du fait que, si cette communication est menée dans l'optique de conférer une aide ou une assistance aux agriculteurs, elle entre dans les prévisions raisonnables de ces derniers[573].

À l'inverse, si les personnes concernées n'ont pu raisonnablement prévoir une telle réutilisation, une base légale est exigée pour déterminer les éléments essentiels du traitement envisagé.

> Ainsi, si elle est menée dans une optique répressive, la communication des données détenues par la DGA à la DGRNE doit être prévue par « une loi, au sens formel du terme, dans ce cas un décret », qui doit prescrire que « la DGRNE peut utiliser à cette fin les données relatives aux agriculteurs provenant du fichier de la DGA qui vise initialement un autre objectif positif dans le cadre de la PAC ; ce décret devra être nécessaire, dans une société démocratique, dans l'intérêt de [...] la sûreté publique [...], de la prévention de troubles et de faits punissables, de la protection de la santé [...] ou de la protection des droits et libertés d'autrui »[574].

---

[572] Voy. l'avis n° 18/2008, *op. cit.*, p. 7, n° 27.

[573] CPVP, avis n° 22/2005 du 21 décembre 2005 relatif à un avant-projet d'arrêté du Gouvernement wallon modifiant le Code de l'eau, l'arrêté du Gouvernement wallon du 12 janvier 1995 portant réglementation de l'utilisation sur ou dans les sols des boues d'épuration et des boues issues de centres de traitement de gadoues de fosses scpetiques et l'arrêté du Gouvernement wallon du 14 juin 2001 favorisant la valorisation de certains déchets, p. 6.

[574] CPVP, avis n° 22/2005, *op. cit.*, p. 7, n° 18.

Un tel raisonnement laisse perplexe. Il pousse à se placer du point de vue du citoyen pour déterminer si l'ingérence doit être encadrée par le pouvoir législatif ou le pouvoir exécutif. Or, cette question doit être déterminée en amont, en fonction du type de traitement et de la menace qu'il constitue pour la protection de la vie privée des personnes concernées[575].

b-2. Une autre question subsiste encore. L'exigence d'un fondement légal ou réglementaire est-elle requise dans le chef de l'administration émettrice ou l'administration destinatrice des données ?

Compte tenu des deux traitements qui constituent une réutilisation de données, il semble qu'il faille exiger l'existence d'une base normative dans le chef de l'administration émettrice des données et une autre dans le chef de l'administration destinatrice de celles-ci.

Pourtant, la CPVP n'analyse pas systématiquement l'existence d'une base légale ou réglementaire dans le chef de l'administration émettrice des données. Ce faisant, certaines communications de données risquent d'être encouragées, alors qu'elles sont effectuées en dehors des missions légalement dévolues aux administrations. Les principes constitutionnels de légalité et de spécialité, traditionnellement applicables à l'action administrative, risquent d'être ébranlés par cette jurisprudence peu scrupuleuse à certains égards[576].

c) Un risque de dérives ? Enfin, le critère des « prévisions raisonnables des intéressés » n'ouvre-t-il pas la porte à des dérives ?

Ce critère est si imprécis qu'on peut lui faire dire ce que l'on souhaite. Il est d'ailleurs surprenant de constater que la jurisprudence de la CPVP est particulièrement fluctuante à ce propos. On sent qu'elle tente de dégager des critères plus concrets au gré des questions qui lui sont soumises en considérant que les prévisions raisonnables sont satisfaites si les personnes concernées ont été suffisamment informées de la réutilisation ou si le traitement ultérieur peut être déduit des termes utilisés dans des dispositions légales.

> Par exemple, à propos du transfert de données entre administrations pour déterminer le montant des allocations pour les personnes handicapées, la CPVP considère que les prévisions raisonnables des intéressés sont respectées car « la législation relative aux allocations de personnes handicapées se réfère

[575] Voy. *infra,* n° 131.-

[576] Voy. not. la délibération du Comité sectoriel Autorité fédérale n° 01/2006 du 14 juin 2006 sur lequel se fonde l'avis n° 49/2006, précité ; CPVP, avis n° 30/2006, *op. cit.,* p. 6, n° 22. Pour de plus amples développements à ce sujet, voy. E. Degrave, « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée », *op. cit.,* pp. 67-69.

> de façon expresse à une condition de revenu, et donc à des données ayant vocation à être de nature fiscale ». Cette notion de revenu « couvre également les revenus provenant de prestations sociales ». Dès lors, la CPVP considère que les traitements ultérieurs de données provenant du SPF Finances et d'administrations de sécurité sociale entrent dans les prévisions raisonnables des personnes handicapées[577].

De telles considérations posent question en pratique. Suffit-il d'informer tous les citoyens que l'on peut effectuer tout type de traitement avec leurs données pour considérer que les prévisions raisonnables des intéressés sont respectées en toute hypothèse ? En d'autres termes, doit-on exiger des citoyens qu'ils consultent et comprennent toutes les normes législatives et réglementaires susceptibles de concerner l'utilisation de leurs données à caractère personnel et, au-delà même de ce qui y est explicitement prévu, d'anticiper les traitements susceptibles de se fonder sur l'interprétation de certains termes utilisés dans ces normes ?[578] À la lecture des avis de la CPVP en la matière, ces questions restent, pour l'heure, sans réponse.

> S'agissant du cas que l'on vient de mentionner, comment peut-on considérer qu'une personne handicapée – ou les personnes en charge de celle-ci – a été à même de prévoir la réutilisation de ces données, souvent sensibles par ailleurs, sur la seule base du vocable « revenu » figurant dans une des multiples législations éparses applicables au statut de ces personnes en difficulté ?

En somme, ces deux critères censés faciliter l'appréciation de la compatibilité entre deux finalités semblent rendre la tâche plus difficile encore. D'ailleurs, lors des discussions préalables à l'adoption de la loi du 11 décembre 1998 qui a modifié la loi du 8 décembre 1992 à l'occasion de la transposition, en droit belge, de la directive 95/46, il a été proposé de supprimer ces deux notions au motif qu'elles étaient « superflues »[579]. L'auteur de l'amendement arguait notamment du fait que les dispositions légales et réglementaires applicables doivent nécessairement être prises en compte pour encadrer l'action de l'administration, sans que la loi du 8 décembre 1992 doive le préciser. Cet amendement a malheureusement été rejeté.

---

[577] CPVP, avis n° 49/2006, *op. cit.*, p. 4, n°s 26 et 27.

[578] Sur l'accessibilité et l'intelligibilité de la loi, voy. E. Degrave, « La légalité pénale et la Cour d'arbitrage », *J.T.*, 2006, pp. 488 et 489 et les références citées.

[579] Projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *Doc. Parl.*, Ch. Repr., sess. 1997-1998, n° 1566/4, pp. 4 et 5 et n° 1566/10, p. 90.

B. La finalité compatible précisée par le législateur

130.- Des critères censés. Malgré les critiques adressées à la manière dont la loi du 8 décembre 1992 organise l'utilisation des critères de compatibilité que sont « les dispositions légales et réglementaires » et « les prévisions raisonnables de l'intéressé », ceux-ci ne sont pas dénués de sens.

Il importe en effet de veiller à ce que l'action administrative respecte les dispositions légales et réglementaires qui encadrent son action. Par ailleurs, l'attention portée aux prévisions raisonnables de l'intéressé rappelle que les échanges de données entre les administrations doivent tenir compte des préoccupations des citoyens et du souci que leur droit à l'autodétermination informationnelle soit respecté.

131.- Des critères à encadrer. Néanmoins, l'appréciation de ces critères, en pratique, ne peut pas être laissée aux administrations. Par exemple, les institutions impliquées dans un échange de données n'ont pas à juger, elles-mêmes, si leur action doit se fonder sur une base légale ou une base réglementaire. En vertu de l'exigence de légalité prévue à l'article 22 de la Constitution, il leur revient seulement de s'assurer que l'échange de données qu'elles veulent effectuer respecte la loi qui régit l'utilisation de ces données.

Elles doivent, par exemple, vérifier que la finalité de cet échange entre dans leurs missions et respecte la finalité déterminée dans ladite loi. Dans le même sens, il ne revient pas aux administrations de déterminer elles-mêmes si la communication de données peut avoir lieu, au travers d'un critère aussi flou que « les prévisions raisonnables des intéressés ». Rappelons en effet que les éléments essentiels du traitement doivent être déterminés par la législateur à qui il revient notamment de définir les destinataires des données réutilisés et le but de la réutilisation opérée.

Partant de là, l'encadrement normatif d'un échange de données et son adéquation par rapport aux prévisions raisonnables des citoyens doivent être réfléchis en amont, par le législateur. Cette affirmation renvoie aux développements qui constituent le troisième chapitre du présent titre. Toutefois, nous précisions d'ores et déjà certains points auxquels le législateur doit être attentif lorsqu'il organise l'e-gouvernement.

§1. Les échanges de données et l'exigence de légalité

132.- Administration émettrice et administration destinatrice. On a évoqué précédemment la question de savoir si l'exigence d'une base légale

ou réglementaire s'adresse à l'administration émettrice des données et/ou à l'administration destinatrice de celles-ci doit.

Pour répondre à cette question, il faut se rappeler qu'un échange de données est constitué de deux traitements distincts et successifs, effectués entre l'émetteur des données[580], d'une part, et le destinataire de celles-ci[581], d'autre part.

Le premier traitement dont question consiste, pour l'instance émettrice des données, à transférer celles-ci à l'instance destinatrice. Il s'agit d'une « communication par transmission » au sens de l'article 1, §2, de la loi du 8 décembre 1992. Le deuxième traitement consiste, pour l'instance destinatrice des données, à recevoir les informations. Il s'agit d'une « collecte de données », au sens de l'article 1, §2, la loi du 8 décembre 1992. Cette collecte est indirecte puisque les données ne proviennent pas directement des citoyens. L'administration émettrice des données et l'administration destinatrice de celles-ci doivent toutes deux agir dans le cadre des missions légales qui sont les leurs et ce, conformément aux exigences de légalité et de spécialité qui s'imposent à l'action administrative. Tant la communication que la collecte des données doivent dès lors être justifiées par une base légale.

D'ailleurs, la CPVP avait suggéré qu'on intègre cette précision dans la loi du 8 décembre 1992, en indiquant explicitement dans la loi que « la communication des données personnelles au sein du secteur public est autorisée pour autant que l'exige l'exécution conforme à la loi des tâches relevant de la compétence à la fois de l'organe qui transmet que de l'organe qui reçoit les donnée »[582]. Le législateur n'a malheureusement pas suivi cette idée, estimant qu'il n'était pas nécessaire d'adopter des règles de protection des données particulière pour le secteur public[583].

133.- Le problème des « vieilles lois ». Une loi adoptée avant l'ère de l'informatique suffit-elle à fonder l'émission ou la réception de données à caractère personnel ? Cette question se pose car la légalité de certains échanges de données au sein de l'administration est justifiée par une loi adoptée avant l'introduction de l'informatique dans l'administration. À notre sens, cette justification est problématique car elle ne tient pas

[580] Il s'agit du département ministériel ou de l'administration qui détient les données réclamées.

[581] Il s'agit du département ministériel, de l'administration qui a réclamé les données transférées.

[582] CPVP, avis n° 7/92 du 12 mai 1992 concernant le projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, p. 27.

[583] Au sujet de l'adoption de règles propres au secteur public, voy. *infra,* n° 174.-

compte du fait que l'informatique n'est pas un moyen comme un autre à la disposition de l'administration.

Deux exemples illustrent cette problématique.

L'article 336 du Code d'impôts sur les revenus prévoit que « Tout renseignement, pièce, procès-verbal ou acte, découvert ou obtenu dans l'exercice de ses fonctions par un agent d'une administration fiscale de l'État, soit directement, soit par l'entreprise d'un des services, administrations, sociétés, associations, établissements ou organismes désignés aux articles 327 et 328 peut être invoqué par l'État pour la recherche de toute somme due en vertu des lois d'impôts ».

Le Commentaire du code des impôts sur le revenu mentionne qu'il se déduit de l'article 336 CIR que « les administrations fiscales de l'État peuvent donc disposer de tous les renseignements d'ordre général ou individuel utiles à l'établissement des impôts considérés dans leur ensemble et se faire mutuellement toute communication dans ce but »[584].

La CPVP a considéré que cette disposition légale justifiait que les données collectées par l'administration du cadastre en vue du remboursement aux personnes concernées d'une taxe indûment payée à l'État belge sur les opérations boursières soient transférées à l'administration de la fiscalité des entreprises et des revenus en vue de contrôler les personnes suspectées de fraude fiscale.

Ce raisonnement ne convainc pas. En effet, une telle possibilité d'échange de renseignements au sein de l'administration fiscale a été octroyée aux administrations fiscales bien avant le développement de l'informatique. La loi du 28 juillet 1938 tendant à assurer l'exacte perception de l'impôt[585] prévoyait déjà, en son article premier, que « les services administratifs de l'État [...] sont tenus, lorsqu'ils en sont requis par un fonctionnaire de l'une des administrations de l'État chargées de l'établissement ou du recouvrement des impôts, de lui fournir tous renseignements en leur possession [...] ». Au moment où elle a été adoptée, le législateur n'avait pas conscience des outils techniques qui « ont donné un aspect tout à fait différent à l'ingérence administrative dans la vie privée du contribuable » si bien qu' « il est permis de se demander si le législateur aurait autorisé les mêmes possibilités d'ingérences dans la vie privée s'il avait connu les moyens techniques actuels »[586]. Depuis lors, cette possibilité d'échanges entre les administrations fiscales n'a pas été réévaluée au regard des technologies nouvelles.

Dans le même sens, on ne peut soutenir que **la loi du 16 novembre 1972 concernant l'inspection du travail** constitue le fondement légal de la

584 *Com. I/R* 336/2.

585 *Pasin.,* 1937-1938, p. 210.

586 P. Glineur, « La fiscalité et l'informatique… vers la naissance d'un droit fiscal de l'informatique », *op. cit.,* p. 79.

communication de données vers le *datawarehouse* OASIS servant à lutter contre la fraude sociale.

Rappelons[587] que cet entrepôt regroupe la copie de centaines de données sociales issues de sources authentiques détenues par le SPF Finances, l'ONSS et l'ONEm ainsi que par le cadastre des investigations. On y applique une opération d'extraction de connaissances appelée *datamining*, afin de dépasser les limites de compétences humaines et effectuer des contrôles sociaux très ciblés. L'enclenchement par le système OASIS de plusieurs alarmes à propos d'un même individu qui est, par conséquent, suspecté de fraude, ne peut pas être assimilé à un « motif raisonnable »[588] justifiant que les inspecteurs sociaux puissent pénétrer à toute heure du jour et de la nuit dans un lieu de travail.

Ce système ne peut pas non plus être justifié par la disposition légale autorisant les inspecteurs sociaux à « rechercher et examiner tous les supports d'information qui se trouvent dans les lieux de travail ou d'autres lieux qui sont soumis à leur contrôle et qui contiennent soit des données sociales [...] soit n'importe quelle autre donnée [...] »[589]. En effet, lorsqu'il a octroyé de telles prérogatives aux inspecteurs sociaux, le législateur n'envisageait pas l'utilisation d'un outil aussi puissant qu'OASIS. Il n'a donc pas examiné la finalité de cet outil, ni la limitation des données enregistrées, et encore moins les responsabilités qu'il induit et les garanties à offrir aux personnes concernées, en termes de transparence notamment. Il en va d'autant plus ainsi que la loi du 16 novembre 1972 a été modifiée en 2006 afin, notamment, de l'adapter « à l'application des technologies informatiques dans les entreprises » sans jamais que soit évoquée l'utilisation d'un entrepôt de données comme OASIS. Les discussions menées se fondent simplement sur l'existence de bases de données constituées par les employeurs[590]. La loi permet aux inspecteurs sociaux d'accéder à celles-ci même si elles n'existent pas en version papier.

Les lois adoptées avant le développement de l'informatique ou sans envisager celui-ci ne peuvent être appliquées telles qu'elles aujourd'hui. Elles organisent des équilibres entre l'administration et les citoyens, qui ont été pensés sans que le législateur ait envisagé la puissance technologique.

Bien que cela puisse constituer un travail d'envergure durant quelques temps, l'article 22 de la Constitution impose d'actualiser les lois anciennes qui permettaient des échanges de renseignements jadis, non en soutenant

[587] Voy. *supra,* n° 44.-

[588] Art. 4, 1° de la loi du 16 novembre 1972.

[589] *Ibid.,* art. 4, c.

[590] Projet de loi portant des dispositions diverses, *Doc. Parl.,* Ch. Repr., sess. 2005-2006, n° 51 2518/001, pp. 154 et s.

qu'elles peuvent, telles quelles, servir de base à des échanges électroniques de données, mais bien en les confrontant aux impératifs de la protection de la vie privée pour redéfinir un équilibre acceptable entre l'administration et les citoyens[591].

> C'est d'ailleurs ce qui a été fait en Suède à l'occasion de la transposition de la directive 95/46. Entre 1998 et 2001, les lois permettant la collecte et l'échange d'informations ont été revues pour les mettre en conformité avec la directive[592].

§2. Les échanges de données et les prévisions raisonnables des intéressés

134.- Un État en réseaux. Comme en témoigne le troisième chapitre, la présente recherche plaide pour l'élaboration d'un « État en réseaux »[593]. Il s'agit d'organiser un e-gouvernement qui se fonde sur une circulation encadrée des données personnelles des citoyens. Pour ce faire, on identifie, au sein du secteur public, plusieurs réseaux sectoriels distincts. Chacun d'eux regroupe des administrations déterminées entre lesquelles les données ont vocation à circuler en principe.

Le critère des prévisions raisonnables des intéressés peut être utile au législateur, au moment de délimiter chaque réseau sectoriel et de déterminer les administrations qui feront partie de ce réseau.

Il revient ainsi au législateur d'identifier les « sphères » de l'administration au sein desquelles le citoyen s'attend à ce que les données circulent. Cela conduit à créer des ensembles, appelés « réseaux sectoriels », regroupant les administrations qui accomplissent des missions complémentaires se rattachant à une même sphère de l'administration de manière à ne pas surprendre le citoyen, ce qui serait le cas si on prévoyait l'échange de données entre des administrations n'étant pas concernées par les mêmes facettes de vie. Ainsi le législateur peut-il créer, par exemple, un réseau sectoriel « taxes et impôts », un réseau sectoriel « emploi », un réseau sectoriel « logement », etc.

---

591 La nécessité d'actualiser les lois au développement des technologies était déjà affirmé par Herbert Burkert en 1983 (« The dimensions of information law », *op. cit.,* pp. 212-213). Dans le même sens, à propos de l'actualisation des lois fiscales, L. VANDEN BERGHE, « Légalité et illégalité dans les échanges de renseignements entre administrations fiscales belges », *R.G.F.,* 1987, p. 179.

592 D. KORFF, « Comparative summary of national laws », *op. cit.,* p. 38.

593 Au sujet de ce modèle d'e-gouvernement, voy. *infra,* n°s 157.- et s.

Dès lors, grâce à la prise en compte par le législateur des prévisions raisonnables des intéressés au moment de définir les réseaux sectoriels et les administrations qui les composent, la structure de l'e-gouvernement sera mieux comprise des citoyens.

135.- Finalités incompatibles. Même si les administrations regroupées dans un réseau sectoriel assurent des missions complémentaires au regard d'un même objectif, certains types de finalités peuvent être d'emblée considérés comme incompatibles. Il est d'ailleurs plus aisé de définir certaines finalités *a priori* incompatibles qu'un ensemble de finalités *a priori* compatibles[594]. Il revient donc au législateur de mentionner clairement ces incompatibilités.

Tel est le cas, par exemple, des échanges de données qui heurtent les prévisions raisonnables d'un citoyen car ils provoquent chez eux le sentiment d'être piégé. C'est pourquoi, le législateur doit à tout le moins interdire qu'une donnée collectée pour satisfaire une finalité avantageuse soit ensuite réutilisée pour une finalité de contrôle.

> Pour cette raison, on ne peut approuver l'avis de la CPVP qui considère que les données collectées par l'administration du cadastre en vue du remboursement aux personnes concernées de la taxe indûment payée à l'État belge sur les opérations boursières peuvent être transférées à l'administration de la fiscalité des entreprises et des revenus en vue de contrôler les personnes suspectées de fraude fiscale. Bien que la finalité de ce traitement ultérieur de données, qui vise une optique répressive, paraisse fort éloignée de la finalité de la collecte de ces données, menée dans une optique favorable aux personnes concernées, la CPVP semble considérer que ce transfert entre dans les prévisions raisonnables des intéressés[595]. Même si l'on comprend le souci de l'État belge de poursuivre les personnes ayant fraudé le fisc, cela ne peut se faire en donnant aux personnes concernées le sentiment d'avoir été piégé.

[594] C'est d'ailleurs ce qu'affirme le Commissariat à la protection de la vie privée du Canada (Commissariat à la protection de la vie privée du Canada, *Le dépistage génétique et la vie privée,* 1995, p. 82 disponible à l'adresse http://www.priv.gc.ca/information/02_05_11_f.pdf). À ce sujet, voy. égal. R. Duaso Calès, *op. cit.,* p. 215.

[595] Avis n° 27/2007 du 19 septembre 2007 relatif à l'échange de données à caractère personnel entre administrations fiscales – vérification fiscale subséquente aux demandes de remboursement de la taxe sur les opérations boursières illégalement perçue suite à l'arrêt de la Cour de Justice des Communautés européennes du 15 juillet 2004.

Section 2. L'exigence de proportionnalité

136.- La notion. L'exigence de proportionnalité est consacrée à l'article 8, §2, de la Convention européenne des droits de l'homme qui affirme que toute ingérence dans le droit à la protection de la vie privée doit être « nécessaire dans une société démocratique »[596].

Cette exigence suppose le respect de deux critères. D'une part, le critère d'*appropriation,* que l'on appelle également le critère de pertinence, consiste à vérifier que la mesure créant l'ingérence dans la vie privée est assez puissante pour atteindre l'objectif visé[597]. D'autre part, le critère de *nécessité* impose de se demander s'il n'existe pas une mesure moins liberticide que celle envisagée, permettant également d'atteindre l'objectif visé[598].

Appliquée à un traitement de données à caractère personnel, l'exigence de proportionnalité désigne le juste équilibre à trouver entre, d'une part, l'ingérence dans la protection de la vie privée provoquée par ledit traitement et, d'autre part, l'objectif poursuivi par celui-ci. Dans l'e-gouvernement, l'objectif visé par un traitement de données est l'efficacité administrative.

137.- L'exigence générale de proportionnalité confortée et renforcée par la protection des données. L'exigence de proportionnalité n'est pas propre au régime de la protection des données. Il existe, en effet, une exigence de proportionnalité que l'on qualifie de « générale », qui s'applique au législateur et aux administrations, même lorsqu'il n'est pas question de données à caractère personnel[599]. Cet impératif signifie que

---

[596] Au sujet de l'exigence de proportionnalité dans la Convention européenne des droits de l'homme, voy. S. Van Drooghenbroeck, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme. Prendre l'idée simple au sérieux,* Bruxelles, Bruylant, Publication des facultés universitaires Saint-Louis Bruxelles, 2001.

[597] S. Van Drooghenbroeck, *op. cit.,* pp. 174 et s. ; B. Renauld et S. Van Drroghenbroeck, « Le principe d'égalité et de non discrimination », *in Les droits constitutionnels en Belgique* (dir. M. Verdussen et N. Bonbled), *op. cit.,* 2011, p. 590.

[598] *Ibid.,* pp. 190 et s.

[599] Parmi la foisonnante doctrine sur le sujet, voy. not. F. Delpérée et V. Bouquey-Remion, « Liberté, légalité et proportionnalité », *A.P.T.,* 1979-1980, pp. 286 à 294 ; P. Martens, « L'irrésistible ascension du principe de proportionnalité », *Présence du droit public et des drotis de l'homme – Mélanges offerts à Jacques Velu,* Bruxelles, Bruylant, 1992, I, pp. 49 à 68 ; E. Ellis (dir.), *The Principle of Proportionnality in the Laws of Europe,* Oxford, Hart Publishing, 1999 ; S. Van Drooghenbroeck, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme. Prendre l'idée simple au sérieux* précité ; B. Renauld et S. Van Drroghenbroeck, « Le principe d'égalité et de non discrimination », *Les droits constitutionnels en Belgique* (dir. M. Verdussen et N. Bonbled), *op. cit.,* 2011, pp. 553 à 605.

« dans la poursuite de politiques qu'elles sont habilitées à mener, les collectivités publiques doivent recourir aux moyens les plus adaptés pour atteindre leur objectif »[600].

Cette exigence générale est confortée et renforcée par la proportionnalité des traitements de données.

a) L'exigence confortée. Le législateur est généralement soumis à une exigence de proportionnalité lorsqu'il prend une mesure qui doit être considérée comme une ingérence dans un droit fondamental. La Cour constitutionnelle le rappelle dans sa jurisprudence constante. Ainsi, lorsque le législateur organise une ingérence dans un droit fondamental, la Cour vérifie qu'il existe « un lien raisonnable de proportionnalité entre le but légitime poursuivi, d'une part, et la limitation des libertés, d'autre part »[601]. En d'autres termes, elle examine l'existence d'un rapport raisonnable entre « les conséquences de la mesure pour la personne concernées et les intérêts de la collectivité »[602].

Le régime juridique de la protection des données conforte l'exigence de proportionnalité traditionnellement applicable au législateur[603], en rappelant que même si le bon fonctionnement d'un État démocratique suppose certaines ingérences dans la vie privée des citoyens, l'efficacité administrative ne justifie pas la mise en place de n'importe quel outil technologique.

b) L'exigence renforcée. Une exigence de proportionnalité est également appliquée aux administrations. Lorsqu'elles ont le choix de leurs moyens d'action, elles doivent veiller à choisir des mesures proportionnées à l'objectif qu'elles poursuivent[604].

Ici, le régime juridique de la protection des données diminue sensiblement le pouvoir des administrations de choisir les moyens de leur action. En effet, comme l'a montré le premier chapitre, il revient au législateur

---

[600] F. Delpérée, *Le droit constitutionnel de la Belgique*, *op. cit.*, p. 594.

[601] Voy. not. C.C., arrêt n° 93/2010, du 29 juillet 2010, B.8. (à propos de la liberté de culte).

[602] Voy. not. C.C., arrêt n° 16/2005, du 19 janvier 2005, B. 5.1. (à propos du droit à la protection de la vie privée).

[603] E. Degrave et Y. Poullet, « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée », *op. cit.*, p. 281.

[604] F. Delpérée et V. Bouquey-Remion, « Liberté, légalité et proportionnalité », *op. cit.,* p. 290 ; M.-A. Flamme, *Droit administratif,* Bruxelles, Bruylant, 1989, p. 485 ; J. Jaumotte, « Les principes généraux du droit administratif à travers la jurisprudence administrative », *in Le Conseil d'État de Belgique – Cinquante ans après sa création (1946-1996),* Bruxelles, Bruylant, 1999, pp. 671-672 ; P. Lewalle, « Le principe de proportionnalité dans le droit administratif belge », *A.P.T.,* 1995, pp. 55 et 74 ; E. Degrave et Y. Poullet, « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée », *op. cit.,* p. 281.

de déterminer notamment les outils de traitements ainsi que les types de données que peuvent utiliser les administrations. Ces moyens d'action à disposition de l'administration sont donc choisis par le législateur, et non les administrations elles-mêmes.

> Par exemple, une administration ne pourrait décider que la mise en place d'une source authentique de données est une mesure proportionnée à l'objectif qu'elle poursuit, ni déterminer les données qui doivent s'y trouver. Cette décision doit être prise et mise en œuvre par le législateur.

Pour le dire autrement, le régime juridique de la protection des données renforce le pouvoir du législateur sur l'administration en lui réservant la compétence de déterminer la proportionnalité des moyens d'action de l'administration.

138.- Deux critères. Comme l'exigence de proportionnalité générale, l'exigence de proportionnalité imposée par le régime juridique de la protection des données suppose le respect des critères d'appropriation et d'efficacité.

Le critère d'appropriation impose de s'assurer que l'outil mis en place est suffisant pour atteindre la finalité poursuivie.

> Par exemple, une base de données ayant vocation à identifier les citoyens à des fins administratives, tel le Registre national, ne serait pas appropriée par rapport à ce but si elle contenait uniquement le nom et le prénom des citoyens, étant donné que des personnes différentes peuvent répondre à ces mêmes données.

Le critère de nécessité aboutit à examiner si la même finalité ne pourrait être atteinte avec un outil créant moins d'atteinte à la protection de la vie privée des personnes concernées par le traitement instauré.

> Par exemple, pour identifier un citoyen, il n'est pas nécessaire de savoir s'il a tenté de contracter un mariage de complaisance[605].

L'examen de l'appropriation du traitement de données par rapport au but poursuivi pose rarement question. Dans l'état actuel de nos recherches, nous n'avons pas connaissance de cas dans lesquels, par exemple, des données trop peu nombreuses ou mal adaptées auraient été demandées rendant le traitement trop peu énergique au regard du but poursuivi. Au

[605] CPVP, avis n° 01/2009 du 14 janvier 2009 relatif à une demande d'avis concernant l'adaptation d'un code dans le type d'information relatif à l'état civil afin de prévenir les mariages de complaisance, n° 19.

contraire, la tendance est plutôt de vouloir accéder à des données trop nombreuses, que l'objectif poursuivi ne justifie pas. C'est pourquoi, l'examen de la nécessité de l'ingérence suscite plus particulièrement le débat lorsqu'il est question d'un traitement de données informatisé.

139.- Proportionnalité du traitement et proportionnalité du contenu du traitement. Outre l'examen de l'appropriation et de la nécessité de la mesure, le régime juridique de la protection des données impose un double examen de proportionnalité. En cela, l'exigence de proportionnalité imposée par le régime juridique de la protection des données est plus précise que l'exigence de proportionnalité générale. Elle exige du législateur un travail paticulièrement minutieux.

D'une part, il y a lieu d'examiner la *proportionnalité du traitement*. Cette exigence n'est malheureusement pas affirmée explicitement par les normes protégeant les données à caractère personnel. En effet, celles-ci imposent une condition de légitimité du traitement.

> Ainsi, l'article 8 de la Charte dispose que « les données doivent être traitées [...] sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi ». La directive 95/46 dresse, en son article 7, la liste des « principes relatifs à la légitimation des traitements de données », que la loi du 8 décembre 1992 a transposés en son article 5.

Or, l'exigence de légitimité du traitement ne fait l'objet d'aucune précision. Partant de ce constat, Marie-Hélène Boulanger, Cécile de Terwangne et Thierry Léonard invitent à se livrer à une interprétation téléologique de la loi pour donner corps à cette exigence. Selon eux, « si le but de la loi est bien de garantir la protection de la vie privée des individus dans notre société, la finalité du traitement et sa mise en œuvre doivent concilier les intérêts de la personne concernée par les données et l'intérêt général ou l'intérêt particulier poursuivi par le responsable du traitement. [...] L'autorité de contrôle et le juge contrôleront cette légitimité sur base de la méthode de pondération des intérêts, reposant sur la règle de proportionnalité »[606]. En d'autres termes, il faut s'assurer que le traitement de données – en l'occurrence, l'outil utilisé par les administrations ou l'utilisation faite des données – est proportionné au but poursuivi.

D'autre part, il importe de veiller à la *proportionnalité du contenu du traitement*, c'est-à-dire à la limitation des données utilisées. En effet, l'article 5, c) de la Convention n° 108 prévoit que les données traitées doivent être « adéquates, pertinentes et non excessives par rapport aux finalités

[606] M.-H. Boulanger, C. de Terwangne et Th. Leonard, *op. cit.*, p. 377.

pour lesquelles elles sont enregistrées ». La directive 95/46 et la loi du 8 décembre imposent une exigence de proportionnalité semblable[607].

I. La proportionnalité du traitement

140.- Deux questions. L'examen de la proportionnalité du traitement suppose la résolution de deux questions.

Un traitement de données est-il nécessaire ?

Dans l'affirmative, comment assurer un juste équilibre entre le but poursuivi et l'immixtion créée dans la vie privée des citoyens ?

A. Un traitement de données est-il nécessaire ?

141.- Endiguer la puissance de l'administration. Les technologies nouvelles ont envahi nos modes de pensées. Aujourd'hui, on se demande rarement s'il est vraiment « nécessaire », au sens de l'article 8 de la Convention européenne des droits de l'homme, de recourir à un moyen informatique. En effet, à la faveur de la multiplication des lois organisant des traitements de données, on semble admettre d'emblée la nécessité des outils technologiques mis au service des missions publiques. Selon Herbert Burkert, « l'expansion des traitements de l'information plutôt que des droits à l'information a – en Europe du moins – été implicitement ou explicitement considérée comme 'nécessaire dans une société démocratique' [...] Ce postulat [...] sous-entend que les évolutions technologiques n'ont pas entamé ni n'entameront la composante démocratique, que les agents de l'État sont en règle générale respectueux de la loi et attachés aux idéaux démocratiques, et que les équilibres en vigueur sont suffisamment solides pour résister à toute tentative de détournement des pouvoirs d'information que le système a par ailleurs déjà mis en place »[608]. Finalement, de manière très regrettable, cela donne l'impression que même « les pères spirituels du droit de la protection des données se sont inclinés devant

[607] Art. 6, c), de la directive 95/46 prévoit que les données traitées doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ». L'article 4, 3°, de la loi du 8 décembre 1992 prévoit que les données traitées doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

[608] H. Burkert, « Progrès technologique, protection de la vie priée et responsabilité politique », *op. cit.*, p. 129.

le fait accompli, à savoir celui que nos données se rencontrent dans des milliers de traitement »[609].

Pourtant, comme nous l'indiquions dans le prélude de l'ouvrage, l'informatisation de l'administration ne peut être banalisée. Elle ne se réduit pas à une « version moderne » des modes traditionnels de gestion des informations relatives aux citoyens. Les technologies rendent l'administration très puissante, ce qui interroge l'équilibre nécessaire entre les pouvoirs de l'administration et ceux du citoyen.

Ce constat doit accompagner le législateur dans l'examen de la proportionnalité du traitement envisagé et convaincre ce dernier d'offrir aux citoyens des garanties nouvelles qui compensent la puissance de l'administration. Dans cette optique, l'examen de nécessité du traitement s'avère fondamental. D'ailleurs, des exemples récents portés devant la CPVP témoignent de l'intérêt de se demander s'il n'existe pas des solutions qui se passent de l'utilisation de données à caractère personnel.

> Les huissiers de justice souhaitaient obtenir un accès au répertoire des véhicules de la DIV en vue « d'identifier l'utilisateur du parking ayant omis de payer le montant dû pour l'utilisation dudit parking ». Faisant application du critère de nécessité, la CPVP s'est montrée défavorable face à cette solution. Elle considère qu'il existe des « méthodes moins intrusives » pour « prévenir les défauts de paiement » et pose la question de savoir « si le gestionnaire [du parking] ne peut/doit l'équiper de barrières ou d'autres systèmes qui empêchent un véhicule de quitter le parking sans paiement »[610].
>
> Dans le même sens, une commune voulait organiser la publicité, par internet, des parcelles de terrain non bâties sur son territoire. Selon la CPVP, une telle publicité est disproportionnée dans la mesure où chaque propriétaire qui désire vendre son terrain en assure lui-même la mise en vente à l'aide des mesures de publicité qu'il choisit[611].

Ces exemples illustrent combien le meilleur moyen d'éviter les abus dans l'utilisation des données des citoyens est de rendre ceux-ci impossibles en empêchant l'accès aux informations protégées. Un outil qui ne nécessite pas l'utilisation de données personnelles demeure mieux adapté

---

[609] P. De Hert, « Chapitre 4. Le droit fondamental à la protection des données à caractère personnel », *in Vie privée et données à caractère personnel* (P. De Hert et D. Pissoort éds.), Bruxelles, Politeia, 2010, pp. 175-176.

[610] CPVP, avis n° 37/2003, *op. cit.*, p. 3.

[611] CPVP, avis n° 40/2006 du 27 septembre 2006 relatif à la tenue des Registres communaux de parcelles non-bâties dont question à l'article 62 du Décret du 18 mai 1999 portant organisation de l'aménagement du territoire et organisation de la publicité par internet via le futur geoloket, p. 8, n° 35.

à cette préoccupation que n'importe quelle mesure de sécurité entourant l'usage des données, celles-ci étant, par essence, toujours faillibles.

142.- Réfléchir à la raison d'être et au contenu de l'intervention législative. Au-delà du souci d'empêcher l'accès aux données des citoyens lorsque ce n'est pas nécessaire, l'examen de la proportionnalité du traitement incite le législateur à réfléchir à la raison d'être et au contenu de son action. Il doit se demander si, finalement, organiser un traitement de données n'est pas pire que bien.

À cet égard, l'échange de données à caractère personnel pour faciliter l'aide aux personnes pauvres, notamment, incite à la réflexion. En témoigne le débat suscité par l'ordonnance bruxelloise du 11 juillet 1991 relative au droit à la fourniture minimale d'électricité[612].

> Cette ordonnance bruxelloise vise à garantir une fourniture minimale d'électricité aux personnes en difficulté financière, dénommés « clients protégés ». Pour ce faire, elle organise un échange de données à caractère personnel entre les entreprises de fourniture d'électricité et la commune.
>
> Concrètement, dès qu'un « client protégé » ne paie pas sa facture d'électricité, l'entreprise d'électricité lui fait parvenir une mise en demeure et, à défaut de paiement dans les 5 jours, place un limitateur de puissance sur le compteur électrique. Dans le même temps, l'entreprise communique son nom à la commune. Celle-ci charge alors le CPAS de procéder à une enquête sociale pour aider l'intéressé à trouver une solution à ses difficultés financières.
>
> Cette procédure repose sur le constat que, bien souvent, le défaut de paiement de la facture d'électricité n'est que le symptôme d'une situation de détresse plus large. Dès lors, tout placement de limitateur de puissance doit être assorti d'un accompagnement social par le CPAS, ce qui justifie, selon le législateur, que l'identité des ménages concernés soit communiquée à la commune.
>
> L'ASBL ATD Quart Monde a attaqué cette ordonnance auprès de la Cour constitutionnelle en invoquant une atteinte à la protection de la vie privée : les données communiquées à la commune ne sont pas de simples données techniques mais révèlent que les personnes concernées relèvent de la catégorie de clients protégés et qu'ils n'ont pas payé leurs factures. La Cour a déclaré le recours infondé, jugeant que l'ingérence, prévue par une « loi », était proportionnée par rapport au but poursuivi[613].

[612] Cette ordonnance est aujourd'hui abrogée et remplacée par l'ordonnance relative à l'organisation du marché de l'électricité en Région de Bruxelles-Capitale, *M.B.,* 17 novembre 2001, qui prévoit une solution semblable.

[613] C.C., n° 14/93, du 18 février 1993.

Dans un tel cas, l'examen de la proportionnalité doit mener le législateur à se poser une question fondamentale : en quoi consiste l'aide aux pauvres ? Comme l'a souligné Olivier De Schutter, « la question de la nécessité et de la proportionnalité de la mesure querellée suppose [...] une connaissance du monde des plus pauvres, dont nul ne peut prétendre avoir le monopole »[614].

En l'occurrence, deux interprétations s'opposent.

Pour la Cour, reprenant les arguments de l'Exécutif de la Région bruxelloise, l'aide aux pauvres suppose que l'on prévienne les situations de détresse en n'attendant pas que les personnes en difficulté demandent de l'aide. Il faut aller vers ces personnes pour réfléchir, avec elles, à des solutions améliorant leur situation.

Par contre, pour l'ASBL ATD Quart Monde, un accompagnement social efficace suppose que l'intéressé en émette le souhait en faisant lui-même la démarche nécessaire. Elle prône un « système inverse à celui qui est prévu, c'est-à-dire : que l'on demande expressément à la personne concernée si elle souhaite que son nom soit transmis au CPAS ou à la commune »[615].

Cette réflexion doit persister en filigrane des lois visant, aujourd'hui, à automatiser, par des flux électroniques de données, les droits de certaines catégories de citoyens, telles que les personnes socialement défavorisées ou les personnes handicapées[616]. Il semble y avoir une tendance à considérer, comme une évidence, que l'aide aux personnes en difficulté suppose nécessairement l'automatisation de leurs droits. Leur situation de faiblesse légitimerait, d'elle-même, l'échange de leurs données à caractère personnel comme s'il n'était pas pensable que ces personnes soient soucieuses de la protection de leur vie privée au point de renoncer à l'octroi automatique d'un droit.

Un postulat si catégorique ne convainc pas. On le constate d'ailleurs actuellement à propos de l'automatisation de l'exonération de la taxe télé-redevance wallonne au profit des personnes bénéficiaires des revenus d'intégration. Une des embûches que rencontre ce projet est l'opposition

---

[614] O. De Schutter, « Observations sous C.A. n° 14/93, du 18 février 1993 », *in* O. De Schutter et S. van Drooghenbroeck, *Droit international des droits de l'homme devant le juge national,* Bruxelles, Larcier, 1999, p. 516.

[615] Conseil de la Région de Bruxelles-capitale, sess. ord. 1990-1991, 14 juin 1991, A-103/2, p. 6, cité par O. De Schutter, « Observations sous C.A. n° 14/93, du 18 février 1993 », *op. cit.,* p. 515, note 19.

[616] Voy., par exemple, la loi-programme du 27 avril 2007 dont le chapitre II organise « l'application automatique de prix maximaux pour la fourniture d'électricité et de gaz naturel aux clients protégés résidentiels à revenus modestes ou à situation précaire », *M.B.,* 8 mai 2007.

de personnes qui « ne désirent pas, et elles l'ont fait savoir, obtenir l'exonération automatique. Elles ne souhaitent pas qu'on utilise leurs données informatiques au niveau de la BCSS »[617]. Il a dès lors été proposé de « mener une investigation avec la BCSS pour s'assurer que, parmi les fichiers transmis, ne figurent pas les personnes qui n'ont pas autorisé la transmission de l'information pour éviter d'avoir un problème supplémentaire avec ces personnes. C'est la raison pour laquelle il n'est pas possible, du jour au lendemain, d'utiliser ce type de fichiers »[618].

Pour s'assurer du besoin réel de recourir à un outil technologique, il pourrait être judicieux d'instaurer une condition de consentement comme garantie procédurale encadrant l'échange de données entre administrations, comme cela a été proposé pour l'exonération automatique de la taxe télé-redevance wallonne. L'effectivité du traitement de données supposerait alors l'accord des personnes concernées.

Par ailleurs, concernant plus particulièrement l'aide aux personnes socialement défavorisées, on doit saluer l'apparition d'un nouveau métier, qui offre de belles promesses. Il s'agit de la fonction d' « expert du vécu »[619]. Ces anciens précarisés ont vécu la pauvreté. Leur rôle est, notamment, d'aider les personnes pauvres dans leurs démarches avec l'administration et de faire part de leurs besoins aux autorités publiques. C'est ainsi que la Banque-Carrefour de la sécurité sociale collabore avec un expert du vécu qui identifie des besoins de simplification administrative dans le but, éventuellement, d'instaurer une automatisation de droits[620]. On peut également imaginer collaborer avec les experts du vécu afin d'améliorer la transparence de l'administration, en ce qui concerne particulièrement les outils à la disposition des citoyens pour introduire des demandes administratives, pour vérifier et mettre à jour leurs données à caractère personnel, pour s'opposer au traitement de leurs informations, etc.[621].

---

[617] Rapport présenté au nom de la Commission du Budget, des Finances, de l'Emploi, de la Formation et des Sports par M. de Lamotte et Mme Barzin, « Présentation de la direction générale opérationnelle de la fiscalité (DG07) », *Doc.,* Parl. w., sess. 2010-2011, n° 288/1, p. 14.

[618] *Idem.*

[619] Pour une évaluation globale de cette fonction nouvelle, voy. T. Van Regenmortel, K. Steenssens, V. Cortese et A. Vanheerswynghels, *Rapport relatif à l'évaluation du projet pilote* « Experts de vécu en matière de pauvreté et d'exclusion sociale au sein des services publics fédéraux » disponible sur le site du SPP-Intégration sociale, mi-is.be.

[620] SPP-Intégration sociale, « Experts du vécu en matière de pauvreté et d'exclusion sociale au sein des services publics fédéraux. De l'expérience individuelle à l'expertise au service des citoyens précarisés », disponible sur le site www.mi-is.be

[621] Sur ces mesures de transparence voy. le Titre II consacré à la transparence de l'e-gouvernement.

B. Le traitement de données réalise-t-il un équilibre entre le but poursuivi et l'immixtion dans la vie privée ?

143.- La mise en balance des intérêts. Si l'on ne peut se passer d'un traitement de données, encore faut-il que l'on mette en balance le but légitime poursuivi par le traitement et l'atteinte de celui-ci sur la protection de la vie privée des personnes concernées.

Cette tâche est délicate en pratique. En effet, on cherche à mesurer des intérêts incommensurables[622]. Comment choisir, par exemple, entre la protection de la sécurité physique des citoyens dans certains lieux publics et la protection de leur vie privée ? Cette incommensurabilité ne rend pas l'appréciation de la proportionnalité impossible, mais elle la pare nécessairement d'une certaine dose de subjectivité[623].

À défaut de pouvoir élaborer une méthode d'analyse susceptible de s'appliquer à tous les cas de figure, les lignes qui suivent tentent de faire émerger certains indices à la lumière d'avis de la CPVP. Il importe de veiller, d'une part, au but poursuivi et, d'autre part, au traitement mis en place.

§1. Le but poursuivi

144.- Un besoin social impérieux. Il a déjà été longuement question du but poursuivi par un traitement de données lors de l'étude de l'exigence de finalité.

Néanmoins, pour saisir pleinement la manière d'apprécier la proportionnalité du traitement de données, il faut préciser ici que la recherche d'un juste équilibre entre le traitement de données et le but visé impose de vérifier que ce but s'assimile à un « besoin social impérieux », comme l'affirment tant la Cour européenne des droits de l'homme[624] que la Cour constitutionnelle[625], la section de législation du Conseil d'État[626] et la CPVP[627].

La notion de « besoin social impérieux » peut être pertinemment illustrée par la problématique du contrôle des citoyens. Nombre de traitements visent, notamment, à lutter contre la fraude fiscale ou à sanctionner

---

[622] S. Van Drooghenbroeck, *op. cit.,* p. 279, n° 388.

[623] *Ibid.,* pp. 281 à 284.

[624] Voy. not. CEDH, *Leander c. Suède, op. cit.*, § 58.

[625] Voy. not. C.C., arrêt n° 131/2005, du 19 juillet 2005, B. 5.1.

[626] Voy. not., l'avis 42.178 du 19 février 2007 sur un avant-projet de loi « relatif aux méthodes de recueil des données des services de renseignement et de sécurité », *Doc. Parl.,* Sénat, sess. 2006-2007, n° 2138/1.

[627] Voy. not. CPVP, avis n° 06/2006, *op. cit.,* p. 7, n° 30.

certaines infractions pénales. De tels objectifs seront considérés comme un besoin social impérieux s'il existe une probabilité suffisamment grande que ces infractions soient commises, comme en témoignent certains avis de la CPVP.

À cet égard, la CPVP s'est prononcée notamment sur la création et l'utilisation d'un entrepôt de données – un « datawarehouse » – permettant des opérations de profilage en matière fiscale[628], et l'accès au registre DIV[629] pour retrouver l'identité du propriétaire d'une voiture impliquée dans un accident de la circulation[630].

> L'utilisation d'un entrepôt de données pour identifier les personnes suspectées de fraude fiscale n'est légitime qu'à certaines conditions. Tout d'abord, « toute prise de décision d'entamer un contrôle sur un contribuable déterminé [...] doit avoir lieu lorsque l'administration dispose de présomptions graves, précises et concordantes selon lesquelles le contribuable a bénéficié de revenus importants qu'il n'a pas déclarés ». En d'autres termes, « une décision d'entamer un contrôle fiscal sur une personne déterminée ne pourra donc être basée uniquement sur le datawarehouse ». En outre, ce traitement de données ne peut être qu'un « outil d'aide à la décision » et « l'intervention des fonctionnaires pour le constat de fraude est [donc] toujours nécessaire »[631].
>
> La communication d'informations de la DIV aux sociétés d'assurance dans le but de retrouver l'identité du propriétaire d'une voiture impliquée dans un accident de la circulation a également été jugée légitime. Selon la CPVP, il s'agit d'une finalité « pour laquelle est indiscutable la supériorité de l'intérêt poursuivi par les assureurs, par rapport à celui des fichés ». Celle-ci « légitime l'interrogation du fichier de la D.I.V. et ce, à partir d'un numéro de plaque précis »[632].

§2. Le type de traitement

145.- Collecte directe et collecte indirecte de données. Pour respecter l'exigence de proportionnalité, il faut choisir un traitement qui assure un équilibre entre, d'une part, le but poursuivi et, d'autre part,

[628] Avis n° 01/2007, précité ; avis n° 16/2007 du 11 avril 2007 relatif à un avant –projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances.

[629] Direction pour l'Immatriculation des Véhicules.

[630] CPVP, avis n° 01/93, *op. cit.,* p. 9.

[631] CPVP, avis n° 01/2007, *op. cit.,* p. 12, n° 67. Dans le même sens, voy. l'avis n° 16/2007, *op. cit.,* p. 7, n° 28 et note 6.

[632] CPVP, avis n° 01/93, *op. cit.,* p. 9, n° 18.

l'autodétermination informationnelle des personnes concernées, en leur garantissant la plus grande maîtrise possible sur leurs informations.

La compréhension de cet impératif fondamental ne peut se passer d'une analyse en fonction des types de traitements existants. Ainsi, une distinction doit être effectuée entre la collecte directe et la collecte indirecte de données. Ces deux types de collecte réalisent des équilibres différents.

La *collecte directe* de données consiste à obtenir les données directement de la personne concernée. Elle permet au citoyen de garder la maîtrise sur les informations qu'il livre à l'administration puisqu'il a connaissance de ce qu'il communique et qu'il livre une information exacte et à jour. Il peut également refuser de divulguer certaines informations, comme l'affirme la CPVP[633]. En pratique toutefois, cette possibilité de refus risque de se réduire à peau de chagrin. On imagine mal, en effet, un citoyen renoncer à une allocation ou à l'octroi d'un permis de bâtir au motif que l'information demandée est excessive.

La collecte directe de données souffre néanmoins d'inconvénients justifiant l'intérêt porté à la collecte indirecte de données dans le développement de l'e-gouvernement. À cet égard, un exemple français incite à la réflexion. Pour faciliter les démarches administratives des citoyens, un service public a été créé par une ordonnance de 2005[634], qui met à leur disposition un « espace de stockage accessible en ligne », ce que l'on pourrait appeler un « coffre-fort électronique ». L'usager peut y conserver les documents utiles à l'accomplissement de ses démarches et peut ainsi plus aisément les communiquer aux autorités administratives qui en ont besoin. Ce système est séduisant car il facilite la communication d'informations aux administrations tout en permettant aux citoyens de garder la maîtrise sur celles-ci. Il faut néanmoins rester attentif au fait que le coffre-fort électronique réalise une centralisation d'un ensemble de données personnelles relatives à un même citoyen. En cas de faille de sécurité, un tiers pourrait y accéder. Par ailleurs, elle requiert du citoyen qu'il sache, d'une part, maîtriser l'usage d'internet pour communiquer avec l'administration et, d'autre part, qu'il veille à répondre aux demandes des administrations.

La *collecte indirecte* de données consiste à obtenir l'information indirectement, c'est-à-dire à partir d'une base de données dans laquelle les informations ont été enregistrées au préalable. Ce type de collecte est encouragé

[633] CPVP, avis n° 20/2008 du 11 juin 2008 concernant l'utilisation de données pour d'autres finalités que celles pour lesquelles elles ont été collectées initialement, p. 6, n° 19.

[634] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, article 7. Voy. à ce sujet, M.-C. Roques-Bonnet, *Le droit peut-il ignorer la révolution numérique ?,* Paris, Michalon, 2010, p. 83.

dans la mise en place de l'e-gouvernement et ce, rappelons-le, pour rendre effectif le principe de la collecte unique des données. Néanmoins, il présente des dangers pour la protection de la vie privée des citoyens car ceux-ci perdent le contrôle de leurs informations. Entre autres risques, la CPVP a souligné que « des données collectées à des fins très différentes sont couplées, de sorte que de nouvelles données concernant la personne concernée apparaissent sans qu'elle n'ait un contrôle sur ce processus »[635].

Compte tenu de la volonté politique, en Belgique, d'encourager la collecte indirecte des données, ce type de traitement retiendra notre attention dans les lignes qui suivent.

146.- Le choix des outils. Pour compenser la perte de contrôle du citoyen sur ses informations, il y a lieu d'assurer à celui-ci certaines garanties qui passent par la mise en place d'outils présentant, en eux-mêmes, des garanties de proportionnalité[636].

La source authentique de données et la plateforme d'échange d'informations offrent des solutions intéressantes pour organiser la circulation des données au sein de l'administration, à la condition de respecter certaines exigences.

1. La source authentique de données

147.- Des informations uniques et fiables. Si différentes administrations doivent accéder aux mêmes données, la source authentique de données est l'outil qui semble le mieux proportionné à cet objectif. Bien qu'elle constitue une menace pour la vie privée puisqu'elle a vocation à assurer la communication des données qu'elle contient, elle est entourée de garanties qui compensent l'immixtion créée dans la vie privée.

Cette base de données d'un type particulier est conçue comme une source unique d'informations fiables. Pareille caractéristique est de nature à assurer un équilibre entre l'efficacité administrative et la protection de la vie privée. C'est pourquoi, elle doit être préférée à la multiplication de bases de données au sein de chaque administration.

En effet, d'une part, grâce à la source authentique, les administrations savent aisément où trouver l'information de qualité nécessaire à l'exécution de leurs missions et ne doivent plus contacter la personne concernée.

---

[635] CPVP, avis n° 20/2008 du 11 juin 2008 concernant l'utilisation de données pour d'autres finalités que celles pour lesquelles elles ont été collectées initialement, p. 6, n° 19.

[636] Le souci de mettre en place des outils présentant en eux-mêmes des garanties de proportionnalité se rattache à la méthode du *Privacy by design,* décrite *infra,* n° 160.-

Elles ne doivent pas non plus s'assurer elles-mêmes de la mise à jour des données, celles-ci étant fiables. L'efficacité administrative est assurée.

D'autre part, en supprimant les copies de fichiers de données à caractère personnel, l'instauration d'une source authentique bénéficie également au citoyen. On évite le risque d'erreurs qui affecte les données qui se trouvent dans des copies de fichiers disséminés dans l'administration, celles-ci n'étant pas ou pas régulièrement mises à jour ou souffrant d'erreurs d'encodage. En outre, on diminue le risque d'accès illégitimes à ces données puisqu'elles ne sont pas enregistrées à plusieurs endroits[637]. Ces garanties doivent être assurées par l'administration responsable de la source authentique. Ainsi, la protection de la vie privée est confortée.

L'effectivité de telles garanties supposent que les données contenues dans une source authentique soient limitées et fiables. Ces exigences sont analysées dans le troisième chapitre.

2. La plateforme d'échanges d'informations

148.- Des échanges de données équilibrés. La plateforme d'échange d'informations[638] répond adéquatement au souci d'organiser l'échange de données entre plusieurs administrations. Bien qu'il constitue une menace pour la protection de la vie privée puisqu'il assure la circulation des informations, cet outil est conçu lui aussi pour réaliser un juste équilibre entre efficacité administrative et protection de la vie privée.

a) Efficacité administrative. La plateforme d'échange d'informations améliore l'efficacité administrative. Grâce à elle, les informations recherchées sont rapidement acheminées vers l'administration demanderesse. La plateforme peut également être un intégrateur de services. En mettant en relation plusieurs sources authentiques, et en usant d'un portail internet convivial, l'intégrateur de services permet aux administrations d' « obtenir des avantages équivalents à ceux d'un enregistrement de données centralisé sans que celui-ci ait effectivement lieu »[639].

> La récente application *Ebirth* témoigne de l'intérêt d'un intégrateur de services pour les administrations. *Ebirth* facilite l'échange des données relatives à la naissance d'un enfant. Ce service part du constat que tant les communes que la Communauté française et le SPF Economie ont besoin d'informations relatives à chaque naissance. Jadis, ces administrations obtenaient

[637] En ce sens, voy. CPVP, recommandation 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public, p. 3.

[638] Sur cette notion, voy. *supra* nos 20.- et s.

[639] CPVP, recommandation 03/2009, *op. cit.,* p. 3, n° 7.

ces informations via des formulaires en papier envoyés par les hôpitaux. Aujourd'hui, les hôpitaux se connectent au portail *Ebirth*, encodent les données requises, et celles-ci sont acheminées respectivement vers les communes, la Communauté française et le SPF Economie, sans que ces institutions doivent accéder à une base de données qui reprendrait toutes les informations, y compris des données inutiles pour leurs missions respectives[640].

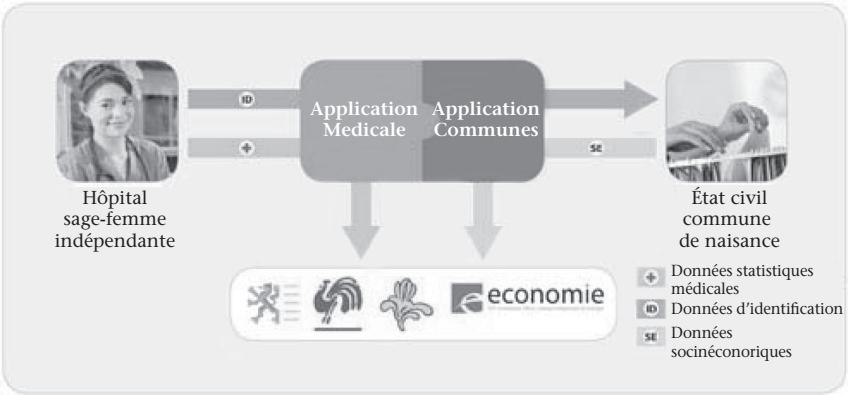

Illustration du service Ebirth, disponible sur le site www.ehealth.fgov.be

b) Respect de la vie privée. La plateforme d'échanges d'informations veille également au respect de la vie privée.

Tout d'abord, cet outil permet aux administrations d'accéder à des données dont elles ne disposent pas, tout en assurant un enregistrement *décentralisé* des informations au sein des sources authentiques. On évite ainsi de centraliser les données dans une seule grande base de données à laquelle toutes les administrations auraient accès.

En cela, la plateforme d'échanges est un outil mieux proportionné que l'intégrateur de données. Cette notion désigne une base de données qui réalise « l'agrégation de données à caractère personnel provenant de plusieurs sources authentiques et leur enregistrement dans une banque de données intégrées distincte, en vue de leurs communication à des tiers »[641]. Comme l'a justement souligné la CPVP, un intégrateur de données représente un danger important pour la vie privée car il s'agit d'une « concentration d'informations à un seul endroit. [...] Il est évident qu'un incident de sécurité concernant une telle banque de données aura un

640 Pour plus d'informations sur *Ebirth*, voy. la présentation générale disponible sur www.ehealth.fgov.be, rubrique services en ligne, *Ebirth*.

641 CPVP, recommandation 03/2009, *op. cit.*, p. 2, n° 2.

impact bien plus important sur la vie privée qu'un incident concernant une des sources d'où les données ont été tirées »[642].

> Il suffirait par exemple qu'un pirate informatique envoie, par internet, un « cheval de Troie » à l'administration détenant la base de données centralisée pour parvenir à prendre possession de toutes les informations s'y trouvant. L'expérience malheureuse dont a récemment été victime le Ministère des Finances français témoigne de ce qu'une telle crainte n'est pas infondée[643]. En outre, la concentration de données augmente le risque qu'un agent, cédant à la curiosité, consulte des données qu'il n'est pas autorisé à connaître dans le cadre de ses missions professionnelles.

Ensuite, la plateforme d'échanges d'informations peut *contrôler* la légalité des accès demandés par les administrations.

C'est ce que fait la Banque-Carrefour de la sécurité sociale en confrontant les demandes de données à la table des autorisations qui fait partie du répertoire des références, afin de s'assurer que l'administration demanderesse a reçu l'autorisation du comité sectoriel compétent pour les données demandées. À cet effet, comme l'a affirmé la CPVP, « travailler avec des répertoires de référence peut contribuer à éviter des consultations illicites »[644].

En cela, la plateforme d'échange est préférable à un système où chaque administration devrait identifier et consulter elle-même la source authentique de l'information recherchée.

> Un tel système est pratiqué aux Pays-Bas, où il existe 13 « basisregistraties » (parmi lesquels un registre « population », placé sous la responsabilité du Ministère de l'Intérieur, un registre « entreprises », placé sous la responsabilité du Ministère des Affaires économiques, un registre « adresses et bâtiments », placé sous la responsabilité du Ministère de l'Infrastructure et de l'environnement, etc.)[645]. Bien qu'un contrôle rigoureux de qualité des don-

[642] *Ibid.,* p. 4, n° 10.

[643] Voy. *supra,* n°s 55.- et s.

[644] CPVP, recommandation n° 03/2009, *op. cit.,* p. 6, n° 17.

[645] Pour de plus amples informations, voy. http://e-overheid.nl/onderwerpen/stelsel-van-basisregistraties/basisregistraties ; http://www.rijksoverheid.nl/onderwerpen/basisregistraties/overzicht-basisregistraties ; P. VAN DER MOLEN, « Authentic Registers and Good Governance », FIG Working Week 2005, disponible à l'adresse http://www.fig.net/pub/cairo/papers/ts_01/ts01_04_vandermolen.pdf ; Y. ELLENKAMP et B. MAESSEN, « Napoleon's registration principles in present times : The Dutch System of Key Registers », 2009, disponible à l'adresse http://www.gsdi.org/gsdiconf/gsdi11/papers/pdf/101.pdf. Ces registres sont soumis à une loi du 9 juin 1994 dénommée « Wet gemeentelijke basisadministratie persoonsgegevens ». En raison de l'existence de cette loi, ces registres ne sont pas soumis à la loi sur la protection de la vie privée hollandaise (Wet bescherming persoonsgegevens, art. 2, d).

nées soit organisé[646], l'inconvénient de ce modèle est de ne permettre qu'un contrôle *a posteriori* de la légalité de l'accès à l'information, par le « College Bescherming Gegevens ». Aucun organisme ne contrôle la communication de l'information avant qu'elle ait lieu.

Enfin, une plateforme d'échanges peut également gérer un réseau primaire et un *réseau secondaire*. L'avantage d'un réseau secondaire est de pouvoir y placer des institutions fondées sur une base idéologique ou politique (telles que les mutuelles ou les syndicats). Ce faisant, l'administration demanderesse et la plateforme n'ont pas connaissance de l'institution auprès de laquelle sont conservées les données recherchées. La plateforme n'a connaissance que du réseau secondaire dans lequel se trouve la donnée recherchée, et est chargée de la demander à l'institution responsable de ce réseau secondaire[647].

II. La proportionnalité des données

149.- La notion de donnée. Selon le Commissariat wallon Easi-Wal – pour « E-administration et SImplification » – la notion de donnée utilisée dans l'administration est définie comme « une information nécessaire à l'administration pour identifier un usager et évaluer sa situation dans un contexte administratif donné »[648].

L'administration n'est toutefois pas libre de choisir, à sa guise, les données répondant à cette définition. En effet, les données utilisées doivent, elle aussi, répondre au prescrit de la proportionnalité. La Convention n° 108 l'affirme explicitement, en prévoyant en son article 5 que « les données à caractère personnel faisant l'objet d'un traitement automatisé sont adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ». La directive 95/46 et la loi du 8 décembre 1992 prévoient une disposition semblable[649].

---

[646] Pour un exemple, voy. le contrôle de la qualité des données du registre « adresses et bâtiments », voy. Ministry of VROM, « Key Registers of Addresses and Buildings », voy. http://inspire.jrc.ec.europa.eu/ref_ser.cfm ?id=32252

[647] Voy. *supra,* n°s 20.- et s.

[648] Easi-Wal, *Formulaires. Guide pour les concevoir et les évaluer,* Namur, Commissariat wallon E-Administration et SImplification, Coll. Guides Pratiques, 2010, p. 7 disponible sur le site http://easi.wallonie.be/servlet/Repository/GPEasiWal_Formulaires.pdf ?IDR=8632

[649] L'art. 6, c) de la directive 95/46 et l'article 4, 3°, de la loi du 8 décembre 1992 prévoient que les données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

Pour répondre à cette exigence, les données utilisées doivent être non seulement limitées, mais également exactes. Ainsi, corollairement à l'examen de la proportionnalité, il importe de s'assurer de la qualité des données, celles-ci devant être exactes et à jour. La qualité des données est étroitement liée à l'exigence de proportionnalité car des données erronées sont nécessairement inadéquates et non pertinentes au regard du traitement effectué. La question de la qualité et de la proportionnalité des données se pose aussi bien lorsqu'une administration veut collecter des informations auprès des citoyens pour créer une base de données à des fins propres, que lorsqu'elle souhaite obtenir communication de données issues d'une source authentique.

A. La qualité des données

150.- Des données exactes et à jour – le devoir de minutie. Les normes régissant la protection des données prévoient, pour la plupart, que les données utilisées doivent être « exactes et si nécessaire mises à jour »[650].

Cette exigence de qualité des informations n'est pas inconnue de l'administration. Elle constitue depuis longtemps une condition essentielle du respect du devoir de minutie traditionnellement applicable à elle. Le devoir de minutie « oblige l'autorité à procéder à une recherche minutieuse des faits, à récolter les renseignements nécessaires à la prise de décision et à prendre en considération tous les éléments du dossier, afin qu'elle puisse prendre sa décision en pleine connaissance de cause et après avoir raisonnablement apprécié tous les éléments utiles à la résolution du cas d'espèce »[651]. Le devoir de minutie suppose donc nécessairement que les informations récoltées et utilisées soient exactes.

Le développement de l'e-gouvernement et les multiples échanges de données ainsi suscités rendent l'exigence de qualité des données particulièrement importante. En effet, une fois la donnée collectée par une

[650] Art. 5, d) de la Convention n° 108 ; art. 6, d) de la Directive 95/46 et art. 4, 4° de la loi du 8 décembre 1992. La directive 95/46 et la loi du 8 décembre 1992 ajoutent que « toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ».

[651] J. JAUMOTTE, « Les principes généraux du droit administratif à travers la jurisprudence administrative », *op. cit.*, p. 687 et les références de jurisprudence citées. Voy. égal. O. DAURMONT et D. BATSELÉ, *op. cit.,* p. 267 ; M. PÂQUES, « L'application de la loi fiscale. Principes de bonne administration en droit administratif et en droit fiscal. Présentation et mise en œuvre », *Act. Droit.,* 1993, pp. 422 à 424.

administration, elle risque d'être échangée de nombreuses fois sans jamais que le citoyen soit amené à en vérifier l'exactitude et à la corriger éventuellement. Si une erreur affecte la donnée échangée, c'est le travail de l'ensemble des administrations l'ayant utilisée qui en pâtit. En clair, une donnée fautive contenue dans une source authentique aura un « effet domino »[652] auprès de toutes les administrations ayant eu communication de celle-ci.

C'est la raison pour laquelle une méticulosité particulière doit entourer la qualité des données enregistrées dans une source authentique. Rappelons que ces données ont vocation à être réutilisées au sein des administrations. Une donnée erronée contenue dans une source authentique créerait beaucoup de dégâts. Dès lors, l'administration auprès de laquelle est créée la source authentique se voit nantie d'une lourde responsabilité. Il lui revient de garantir la fiabilité des données[653]. C'est pourquoi, la CPVP recommande de ne pas enregistrer des données qui ne sont pas suffisamment stables, afin d'éviter les coûts de mise à jour et les risques d'erreurs.

> Cela explique, par exemple, que la CPVP se montre défavorable à l'enregistrement de la donnée « profession » au Registre national au motif que cette information n'est pas systématiquement mise à jour étant donné que peu de gens déclarent leur changement de profession[654].

En outre, l'obligation de l'administration responsable de la source authentique de garantir la fiabilité des données doit se concevoir comme une obligation de résultat à laquelle doit correspondre une présomption de responsabilité de l'administration en cas d'erreur affectant la donnée[655].

---

[652] CPVP, avis n° 11/2009 du 29 avril 2009 concernant le projet d'arrêté du Gouvernement flamand portant exécution du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, p. 3, n° 6.

[653] La garantie de fiabilité des données suppose nécessairement l'implication des personnes concernées par celles-ci et qui fera l'objet d'une analyse dans le chapitre 2 sur la transparence.

[654] CPVP, avis n° 19/2002 du 10 juin 2002 relatif au projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, au projet d'arrêté royal relatif aux cartes d'identité et au projet d'arrêté royal portant mesures transitoires en ce qui concerne la carte d'identité électronique en Belgique, p. 3 ; CPVP, avis n° 12/2003 du 13 janvier 2003 relatif au projet d'arrêté royal déterminant les informations techniques associées aux informations visées à l'article 3, alinéa 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques », p. 3 ; CPVP, avis n° 39/2003 du 25 septembre 2003 relatif au projet d'arrêté royal déterminant les informations techniques associées aux informations visées à l'article 3, alinéa 1er, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, p. 3.

[655] Voy. *infra,* n° 218.-

B. La limitation des données

151.- Les missions légales de l'administration et la finalité du traitement. L'exigence de proportionnalité impose de limiter l'utilisation des données par rapport aux missions légales de l'administration. Pour ce faire, il faut prendre en compte les normes législatives et réglementaires définissant les tâches de l'administration.

Par ailleurs, il s'impose également de limiter les données en fonction de la finalité précise poursuivie par le traitement de données. À la faveur du développement des technologies permettant le traitement de données se dégagent des solutions nouvelles. Dans les lignes qui suivent, on se penchera sur deux d'entre elles : la limitation des données à la mention « oui-non » lors d'un échange d'informations et la limitation des données lors de leur enregistrement dans une source authentique.

En guise d'illustration, le choix est fait de se concentrer sur l'utilisation, au sein de l'administration, des données relatives au revenu des citoyens. Cette problématique intéresse beaucoup d'institutions. En effet, nombreuses sont les administrations qui souhaitent accéder à des données de revenu détenues par la SPF Finances afin d'octroyer automatiquement une réduction aux personnes qui y ont droit, ou pour calculer l'exact montant de l'allocation demandée lorsque celle-ci dépend des ressources effectives de la personne qui la réclame, ou encore, pour récupérer certaines créances. Pour cette analyse, on se fonde sur certaines décisions du Comité sectoriel de l'Autorité fédéral, qui est l'autorité compétente pour autoriser la communication de données émanant du SPF Finances.

§1. La limitation des données par les textes légaux et réglementaires définissant les missions de l'administration

152.- Le besoin réel de l'administration. L'administration ne peut collecter que des informations auxquelles elle a le droit d'accéder en vertu des normes en vigueur. C'est pourquoi, il est conseillé de se demander si les informations dont l'utilisation est envisagée répondent à un « besoin réel »[656] de chaque administration. À nouveau, il s'agit d'une application du principe de la spécialité des administrations. Celles-ci ne pourraient, à l'occasion d'un traitement de données, accéder à des informations qui ne sont pas nécessaires pour exercer leur mission.

[656] Easi-Wal, *Formulaires. Guide pour les concevoir et les évaluer,* Namur, Commissariat wallon E-Administration et SImplification, Coll. Guides Pratiques, 2010, p. 7 disponible sur le site http://easi.wallonie.be/servlet/Repository/GPEasiWal_Formulaires.pdf ?IDR=8632

Dans cette optique, le Comité sectoriel vérifie si un texte légal ou réglementaire justifie que l'administration demanderesse accède aux données réclamées.

> Ainsi, le Comité sectoriel a-t-il affirmé que « les données de revenus demandées doivent toujours rester limitées à ce qui est nécessaire à l'application des règles en vigueur »[657]. Par exemple, à propos de l'accès à des données du SPF Finances pour contrôler le montant du revenu des personnes demandant l'octroi d'avantages liés au statut OMNIO, le Comité sectoriel a admis, à plusieurs reprises, que les données réclamées étaient adéquates, pertinentes et non excessives en considérant que celles-ci sont « requises pour déterminer aussi précisément que possible les revenus annuels bruts des personnes concernées » en mentionnant la disposition de la loi ou de l'arrêté royal précisant la nécessité de se référer à un tel revenu pour octroyer l'avantage en question et prévoyant le contrôle des données communiquées par les personnes concernées[658]. Il a justifié sa décision en soutenant que « chaque donnée concerne un élément de revenus qui peut être lié soit à un code déterminé sur le formulaire de déclaration tel qu'introduit par la personne concernée[659], soit à un calcul que le fisc a réalisé sur la base des informations fournies sur le formulaire de déclaration (par exemple, la personne concernée remplit le revenu cadastral et c'est le fisc qui veille à l'indexation afin de déterminer la valeur actuelle de ce revenu) »[660].

---

[657] C.S.A.F., Délibération n° 14/2009, du 1er octobre 2009, relative à une demande d'autorisation de la « Vlaamse Maatschappij voor Sociaal Wonen (Société flamande du logement social) pour le traitement de données à caractère personnel enregistrées dans des banques de données du Service public fédéral Finances », p. 10, n° 23.

[658] Par exemple, concernant l'intervention d'assurance majorée liée au statut OMNIO notamment, il s'agit de l'article 24 de l'arrêté royal du 1er avril 2007 fixant les conditions d'octroi de l'intervention majorée de l'assurance visée à l'article 37, §§ 1er et 19 de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, et instaurant le statut OMNIO. Voy. la délibération AF n° 02/2008 du 14 février 2008 relative à une demande formulée par l'INAMI en vue d'obtenir la communication de données à caractère personnel par le SPF Finances concernant les revenus de titulaires de l'intervention majorée de l'assurance inscrits au Registre national, p. 6, n° 18.

[659] Nous précisons qu'il s'agit du formulaire de déclaration, prévu par les textes applicables, qui imposent aux personnes qui demandent ces avantages de faire une déclaration sur l'honneur du montant de leurs revenus et d'accompagner cette déclaration de preuves. Cette déclaration est ensuite contrôlée par l'INAMI, ce qui est également prévu par les textes applicables. Voy., par exemple, les articles 26 et 45 de l'arrêté royal du 1er avril 2007 fixant les conditions d'octroi de l'intervention majorée de l'assurance visée à l'article 37, §§ 1er et 19 de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, et instaurant le statut OMNIO.

[660] Délibération AF n° 01/2008 du 14 février 2008, relative à une demande formulée par l'INAMI en vue d'accérder à des données à caractère personnel du SPF Finances dans le cadre de l'application du statut OMNIO, p. 6, n° 24 ; Délibération AF n° 02/2008 du 14 février 2008 relative à une demande formulée par l'INAMI en vue d'obtenir la communication de données à caractère personnel par le SPF Finances concernant les revenus de

L'obligation d'utiliser les données à caractère personnel conformément aux textes légaux et réglementaires applicables à l'administration explique que l'administration soucieuse de déterminer le revenu exact des personnes concernées n'a pas nécessairement accès aux données de revenu de toutes les personnes *a priori* concernées.

> Par exemple, en vertu de l'arrêté royal du 25 novembre 1991 portant réglementation du chômage, un chômeur peut exercer une activité rémunérée non salariée, tout en percevant des allocations de chômage. Toutefois, si tel est le cas, les allocations de chômage sont réduites en conséquence.
>
> Pour connaître avec certitude le montant des revenus perçus dans le cadre de cette activité rémunérée, l'ONEm a demandé au Comité sectoriel pour l'Autorité fédérale de pouvoir accéder à certaines données relatives aux chômeurs, détenu au SPF Finances. Le Comité sectoriel a jugé que les données réclamées étaient adéquates, pertinentes et non excessives mais qu'elles ne pouvaient pas être demandées concernant tous les chômeurs. En effet, la disposition réglementaire prévoyant la réduction des allocations de chômage en cas d'exercice d'une activité rémunérée ne s'applique pas à tous les types de revenus. Par exemple, elle ne s'applique pas lorsque l'activité rémunérée est l'exercice d'un mandat de conseiller communal. C'est pourquoi, le Comité sectoriel conclut qu'« à défaut d'harmonisation des notions légales de [...] montant de rémunération devant être pris en compte en application de la réglementation du chômage, il appartient à l'ONEm d'adapter les formulaires de déclaration sur l'honneur de manière telle que les chômeurs déclarent expressément si, oui ou non, ils perçoivent des revenus exclus de la notion de rémunération au sens de la réglementation du chômage [...]. Ainsi, les fonctionnaires en charge de la gestion administrative seront à même d'apprécier, préalablement au cas par cas, au vu de la nature de l'activité non salariée exercée par le demandeur d'allocation de chômage, si l'article 130 de l'AR précité du 25 novembre 1991, rendant la collecte des données fiscales pertinentes et nécessaire pour la finalité précitée, est d'application »[661].

---

titulaires de l'intervention majorée de l'assurance inscrits au Registre national, p. 7, n° 21 ; Délibération AF n° 09/2008 du 20 novembre 2008 relative à une demande des organismes assureurs de mise en place de flux électroniques de données relatives aux revenus perçus par les assurés sociaux ayant demandé le bénéfice du statut PMNIO entre eux et le SPF Finances ainsi qu'entre 77 mutualités et le SPF Finances, p. 11, n° 24.

[661] Délibération AF n° 03/2008 du 3 juillet 2008 relative à la demande de l'ONEm de se voir communiquer par voie électronique du SPF Finances des données relatives aux revenus des demandeurs d'allocations de chômage pour les finalités de détermination et d'actualisation du montant de l'allocation de chômage devant être réduit à la suite de la perception d'allocations de chômage cumulée avec l'exercice d'une activité lucrative non salariée, pp. 9 et 10, n°s 23 et 24. Dans le même sens, voy. la délibération AF n° 04/2008 du 3 juillet 2008 relative à la demande de l'Onem de se voir communiquer du SPF Finances par voie électronique des données relatives aux revenus des demandeurs d'allocation de chômage pour vérifier le caractère accessoire d'une activité exercée par un chômeur de manière complé-

Le respect de l'encadrement normatif applicable à l'administration explique également qu'une institution n'a pas nécessairement accès aux données de revenu les plus récentes. C'est le cas lorsque les textes ne l'exigent pas.

> Par exemple, pour certaines catégories de bénéficiaires de l'allocation de chauffage, la législation impose de tenir compte des revenus de l'année civile précédant celle au cours de laquelle la demande d'allocation de chauffage est introduite. Dès lors, le Comité sectoriel a décidé que « lors du contrôle visant à déterminer si l'intéressé fait ou non partie d'une de ces catégories, les CPAS ne peuvent utiliser que les données relatives aux revenus qui sont visées par la législation » et non « les données les plus récentes » comme ils le demandaient[662].

§2. La limitation des données par la protection de la vie privée

153.- La finalité du traitement. La protection de la vie privée ne se contente pas du respect du principe de spécialité. Elle impose de rester attentif à la finalité précise poursuivie et de limiter les informations à l'accomplissement de celle-ci.

C'est pourquoi, il suffit parfois de ne communiquer qu'une mention « oui-non ».

Par ailleurs, les données contenues dans une source authentique doivent faire l'objet d'une limitation particulière.

---

mentaire avec la perception d'allocation de chômage, p. 10, n°s 26 et 27 ; délibération AF n° 05/2008 du 3 juillet 2008 relative à la demande de mise en place, entre l'ONEm et le SPF Finances, d'un flux électronique de données à caractère personnel relatives aux revenus dont disposent les chômeurs pour la finalité de contrôle, par les inspecteurs sociaux de l'ONEm, de l'exactitude et de la complétude des déclarations sur l'honneur des chômeurs relatives à leurs revenus influençant le droit aux allocations de chômage, p. 11, n° 23 ; Délibération AF n° 06/2008 du 3 juillet 2008 relative à la demande de mise en place, entre l'ONEm et le SPF Finances, d'une flux électronique de données relatives aux revenus perçus par les personnes avec lesquelles les chômeurs cohabitent, afin de permettre aux inspecteurs sociaux de l'ONEm de contrôler l'exactitude et la complétude des déclarations sur l'honneur pour vérifier la catégorie familiale à laquelle appartient le chômeur, dont question à l'article 110 de l'AR du 25 novembre 1991 portant réglementation du chômage, p. 11, n° 25.

[662] Délibération AF n° 07/2008 du 31 juillet 2008 relative à une demande d'obtention d'un accès électronique à des des données conservées actuellement par le SPF Finances en vue de la réalisation d'une enquête sociale par les CPAS dans le cadre de l'octroi d'allocations de chauffage, pp. 9 et 10, n° 35. Voy. également la délibération AF n° 01/2008, *op. cit.*, p. 6, n°s 26 et 27.

1. La limitation des données à la mention « oui-non »

154.- La mention « oui-non ». Les réflexions menées principalement à la faveur du développement de la Banque-Carrefour de la sécurité sociale et de l'utilisation de la donnée « revenus », ont fait émerger un critère de limitation des données intéressant. Nous l'appelons la mention « oui-non ».

Pour comprendre cette notion, il y a lieu de constater qu'un texte légal ou réglementaire fondant la collecte des données n'est pas, en lui-même, une preuve suffisante de la proportionnalité des données réclamées. En effet, l'exécution de certaines missions ne nécessite pas la connaissance du montant exact du revenu de la personne concernée. L'indication que cette personne dépasse ou non un certain seuil de revenus suffit, peu importe le montant exact de celui-ci. Dans cette hypothèse, il n'y a dès lors pas lieu d'accéder aux multiples informations permettant de calculer le revenu des personnes concernées.

En quoi consiste la mention « oui-non » ? Lorsqu'une administration a besoin de connaître le revenu d'une personne, la mention « oui-non » consiste à se demander s'il est nécessaire de communiquer à l'administration le montant exact du revenu de cette personne ou s'il lui suffit de savoir si la personne dépasse ou non le seuil requis par la législation pour obtenir l'avantage qu'elle réclame ou pour se voir imposer le paiement de la taxe à laquelle elle est soumise. Dans ce second cas de figure, l'administration émettrice communique un « oui » ou « non », qui est la réponse à la question « telle personne dépasse-t-elle tel seuil de revenu ? ».

> Par exemple, la Société flamande du Logement social voulait obtenir, de la part du SPF Finances, le montant du revenu soumis à l'impôt des personnes physiques de certaines personnes souhaitant une aide pour se loger, tels que les candidats emprunteurs d'un prêt social. Le Comité sectoriel a constaté que « pour entrer en ligne de compte pour un prêt social, une limite minimale et maximale de revenus est fixée »[663] et a affirmé que « le demandeur n'a [...] pas besoin lui-même de toutes les donnés détaillées pour poursuivre dans ce contexte (ces) finalités [...] mais doit généralement à ce stade uniquement pouvoir déterminer si les revenus de la personne concernée se situent ou non sous un certain seuil ». Dès lors, il a recommandé à cette institution « d'élaborer un système par lequel le demandeur ne reçoit une réponse qu'à la question de savoir si cette condition de revenus est respectée ou non.

[663] Délibération AF 14/2009, du 1er octobre 2009, relative à une demande d'autorisation de la « Vlaamse Maatschappij voor Sociaal Wonen (Société flamande du logement social) pour le traitement de données à caractère personnel enregistrées dans des banques de données du Service public fédéral Finances », p. 4, n° 10.

> Ainsi, le demandeur n'a pas accès à toutes les données de revenus détaillées qui sont conservées au SPF Finances, ce qui donnerait évidemment lieu à un traitement de données plus proportionnel »[664].

Cette solution se répand de plus en plus. Elle est, par exemple, utilisée pour octroyer la réduction forfaitaire relative à la fourniture de gaz naturel, d'électricité et de mazout. Le SPF Economie n'accède pas à « un aperçu détaillé des revenus du demandeur », il « ne reçoit qu'une réponse positive ou négative à la question de savoir si le demandeur de la réduction répond ou non à la condition de revenus ». Ce faisant, il « ne reçoit pas d'autres données que celles strictement nécessaires »[665].

Cette solution a également été prônée concernant l'évaluation des conditions justifiant l'octroi du statut OMNIO[666].

155.- Une solution pertinente. Il y a lieu de saluer la pertinence de ce mécanisme et d'encourager son utilisation pour toutes les collectes de données chaque fois qu'il n'est pas nécessaire de connaître l'exacte ampleur des ressources de la personne concernée. On pourrait également imaginer l'appliquer à d'autres données que le revenu. Ce pourrait être le cas, par exemple, lorsqu'il faut savoir si un citoyen a plus de x enfants, ou a plus de tel âge, etc. On peut répondre « oui » ou « non » sans communiquer la mention du nombre exact d'enfants ou l'âge exact de la personne concernée.

L'application de la mention « oui-non » à l'action administrative est intéressante car elle balise l'utilisation des technologies en empêchant une institution d'accéder à des données auxquelles elle n'a pas le droit d'accéder, évitant ainsi les immixtions injustifiées dans la vie privée des citoyens.

---

[664] *Ibid.*, n° 24.

[665] Délibération AF 11/2008, du 18 décembre 2008, relative à la transmission de données à caractère personnel du SPF Finances au SPF Économie, PME, Classes moyennes et Énergie, via la Banque-Carrefour de la Sécurité sociale, en vue de l'octroi d'une réduction forfaitaire pour la fourniture de gaz naturel, d'électricité et de mazout, p. 9, n°s 28 et 29. Voy. également la délibération AF 08/2008, du 11 août 2008, relative à la transmission de données à caractère personnel du SPF Finances à la Banque-Carrefour de la Sécurité Sociale et de la Banque-Carrefour de la Sécurité Sociale au SPF Économie, PME, Classes moyennes et Énergie, en vue de l'octroi d'une réduction forfaitaire pour la livraison de gaz et d'électricité ; délibération AF n° 09/2008, *op. cit.*, n° 27.

[666] Délibération AF 09/2008, du 20 novembre 2008, relative à une demande des organismes assureurs de mise en place de flux électroniques de données relatives aux revenus perçus par les assurés sociaux ayant demandé le bénéfice du statut OMNIO entre eux et le SPF Finances ainsi qu'entre 77 mutualités et le SPF Finances.

Ce mécanisme illustre le fait que l'utilisation des technologies peut protéger davantage la vie privée des citoyens que le font les textes légaux et réglementaires qui encadrent l'octroi de ces avantages ou l'imposition de ces taxes[667]. En effet, une collecte indirecte de données limitée à une réponse sous forme d'un « oui » ou d'un « non » permet à l'administration demanderesse de l'information d'effectuer sa mission consistant à évaluer si elle doit, ou non, octroyer l'avantage en question à telle personne, tout en n'accédant pas à toutes les données auxquelles elle peut pourtant accéder en vertu des textes qui encadrent son action mais qui s'avèrent disproportionnées au regard de la protection de la vie privée.

2. La limitation de la durée de conservation des données

156.- Durée de conservation et missions légales. L'exigence de proportionnalité implique également, comme l'affirment la directive 95/46 et la loi du 8 décembre 1992, que les données à caractère personnel soient conservées « pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement »[668].

Appliquée au secteur public, la durée de conservation des données par une administration sera fonction de la nécessité des données au regard des missions légales à accomplir. Une fois celles-ci réalisées, les données deviennent inutiles et doivent être détruites.

> Par exemple, lorsque les données sont nécessaires pour examiner le droit à l'obtention d'une allocation, l'administration chargée du paiement de celle-ci peut généralement conserver les données d'identification des personnes concernées durant le délai de prescription de l'action en recouvrement de l'indu. Celui-ci est, bien souvent, de 5 ans[669]. En effet, durant ce délai, l'administration doit pouvoir vérifier la légalité de son action et éventuellement rectifier les erreurs commises en contactant la personne ayant bénéficié indûment du paiement d'une allocation. Il a déjà été admis que l'administration conserve les données durant une année supplémentaire par rapport au délai

[667] Au sujet de la protection de la vie privée par la technologie, voy. *infra,* n°s 159.- et s.

[668] Art. 6, 1., e), de la directive 95/46 ; art. 4, 5°, de la loi du 8 décembre 1992. Pour une application de l'exigence de proportionnalité à la durée de conservation des données d'identification des personnes ayant accédé à une base de données, voy. C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 7 mai 2009*, College van burgemeester en wethouders van Rottredam c. m.e.e. Rijkeboer*, aff. C-553/07, *R.D.T.I.,* 2011, pp. 79 et 80.

[669] Voy. not. Délibération AF n° 01/2008, *op. cit.,* p. 7 ; délibération AF n° 02/2008, *op. cit.,* p. 7.

légal de prescription au motif que celle-ci est « recommandée pour permettre un contrôle et pour être certain que la prescription a totalement expiré »[670].

Autre exemple, les données issues du registre de la DIV nécessaires pour identifier les personnes qui sont débitrices, du fait de l'utilisation d'un véhicule, d'une redevance de stationnement ne peuvent pas être conservées après le paiement de la redevance. Cela reviendrait, en effet, à constituer une base de données parallèle à celle de la DIV[671].

*

Conclusions

La finalité et la proportionnalité sont deux exigences cardinales qui s'imposent à tout traitement de données à caractère personnel. Le législateur doit s'y soumettre lorsqu'il rédige une loi qui encadre l'e-gouvernement.

La finalité doit être déterminée, explicite et légitime, ce qui conforte le principe de spécialité émanant du droit administratif et même, le renforce. En outre, amené à déterminer une finalité précise, le législateur doit réfléchir à la raison d'être de la politique menée, et l'indiquer clairement dans la loi.

La compatibilité de la finalité de réutilisation des données avec celle de leur collecte est également primordiale dans l'e-gouvernement, puisque la collecte unique des données suppose la circulation de celles-ci au sein de l'administration. Tentant d'interpréter cette notion floue, nous avons notamment insisté sur l'importance, pour le législateur, de rester attentif à l'exigence de légalité et de ne pas trop rapidement tolérer que des traitements de données se fondent sur des lois obsolètes, adoptées avant l'ère de l'informatique. L'intérêt du critère des « prévisions raisonnables des intéressés » a également été souligné s'agissant de la délimitation des réseaux sectoriels.

Par ailleurs, l'exigence de proportionnalité impose un double examen au législateur. La proportionnalité du traitement doit le mener à choisir l'outil le moins attentatoire à la vie privée des citoyens. La proportionnalité des données lui impose d'autoriser l'utilisation des seules données pertinentes, adéquates et exactes.

---

[670] Voy. not., Délibération AF n° 07/2008, *op. cit.,* p. 10, n° 38.

[671] Voy. not. délibération AF 12/2009 du 1er octobre 2009 portant autorisation unique pour l'acès au répertoire de la DIV à des fins d'identification des personnes qui sont débitrices, du fait de l'utilisation d'un véhicule, d'une rétribution, taxe ou redevance de stationnement, p. 7, n° 37.

Grâce à ces exigences et à l'interprétation qu'elles reçoivent de la part de la CPVP, le législateur est utilement guidé dans la tâche qui lui revient, celle d'encadrer l'e-gouvernement.

En cela, les exigences de finalité et de proportionnalité permettent au législateur de garder une maîtrise de l'administration, bien que l'e-gouvernement rende cette tâche plus difficile, comme l'a montré le premier chapitre. On peut affirmer qu'en aidant le législateur, le régime juridique de la protection des données contribue au respect de l'exigence de légalité dans le contexte de l'e-gouvernement.

Fort de ces enseignements, le législateur doit à présent se mettre à l'œuvre pour organiser un e-gouvernement qui respecte les exigences constitutionnelles imposées par l'article 22 de la Constitution, ainsi que les diverses obligations qui découlent du régime juridique de la protection des données à caractère personnel. Le troisième chapitre s'y consacre.

*

CHAPITRE III.
L'organisation d'un e-gouvernement légal

Introduction

Comme l'ont souligné les deux premiers chapitres, l'organisation de l'e-gouvernement laisse aujourd'hui apparaître deux failles majeures. D'une part, la structure de l'e-gouvernement est peu homogène et difficilement compréhensible pour les citoyens. Elle est fondée sur des outils de traitements de données qui sont mis en place de manière parsemée, au service de certaines administrations seulement. D'autre part, l'e-gouvernement est encadré par des règles éparses et floues, parmi lesquelles certaines n'ont pas été soumises à un réel débat démocratique alors qu'elles mettent en jeu la protection de la vie privée des citoyens. Certaines de ces règles ne respectent pas non plus le prescrit des normes nationales et supranationales organisant la protection des données à caractère personnel et, en particulier, les exigences de finalité et de proportionnalité des traitements de données.

Un tel constat heurte l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et la directive 95/46. Les deux premiers chapitres se sont attachés à le montrer.

Pour résoudre ces écueils, deux voies peuvent être suivies.

Dans un premier temps, il convient de réfléchir à la structure de l'administration et de choisir un modèle d'e-gouvernement cohérent et compréhensible, qui respecte l'exigence de légalité et les règles de protection des données. Cela suppose qu'on prenne du recul et qu'on renonce à organiser l'e-gouvernement au gré de l'apparition des nouveaux outils technologiques comme on a eu tendance à le faire jusqu'à présent. D'aucuns ont souligné l'importance d'un tel choix[672]. Les fondements de l'e-gouvernement ne s'apparentant pas à ceux de l'administration papier, ils doivent être réévalués dans leur ensemble. Cela ne suppose pas seulement la mise en place

[672] P. TRUDEL, « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », *op. cit.*, p. 258 ; T. WÜRTENBERGER et G. SYDOW, « Administration électronique et protection de la vie privée en Allemagne », *in L'administration électronique au service des citoyens. Actes du colloque organisé par le Conseil d'État et l'Université Paris I Panthéon Sorbonne à Paris, les 21 et 22 janvier 2002* (dir. G. CHATILLON et B. DU MARAIS), Bruxelles, Bruylant, 2003, pp. 368-370 ; E. LAU, « Principaux enjeux de l'administration électronique dans les pays membres de l'OCDE », *Rev. Fr. Adm. Publ.*, 2004, p. 229.

adéquate d'outils technologiques mais « des changements organisationnels et culturels plus profonds au sein des administrations publiques dont la collaboration est indispensable au développement d'une orientation vers le client [...] »[673]. Dans un rapport rendu il y a quelques années sur l'administration électronique, plusieurs parlementaires ont affirmé la même volonté, soutenant que « la solution consistant à rendre lesdits services accessibles par l'intermédiaire des TIC ou à copier électroniquement les procédures actuelles est tout à fait insuffisante. L'e-gouvernement ne deviendra une réalité que lorsque les services auront été redessinés dans leur ensemble »[674].

> La section de législation du Conseil d'État se prononçait déjà en ce sens il y a quinze ans en affirmant que « la phase expérimentale de la loi du 8 décembre 1992 peut être considérée comme révolue »[675] et que, dès lors, certaines règles devaient être réévaluées.

Une fois ce modèle choisi, il convient, dans un deuxième temps, d'adopter des règles claires et adaptées aux enjeux de l'e-gouvernement.

Les lignes qui suivent sont consacrées, dans une première section, à la structure de l'e-gouvernement. Une deuxième section détaille la tâche du législateur, à qui il revient d'encadrer l'e-gouvernement par l'adoption de lois particulières, d'une loi-cadre et d'accords de coopération.

*

Section 1. La structure de l'e-gouvernement

157.- Considérations générales. Comme on l'a dit à de multiples reprises, l'e-gouvernement doit être structuré selon un modèle qui réponde à deux impératifs : la protection de la vie privée et l'efficacité administrative. Ces impératifs doivent être envisagés très tôt, dès le moment où l'on définit le modèle d'e-gouvernement dans lequel on souhaite s'engager, car ils conduisent à choisir certains outils de traitements plutôt que d'autres.

---

[673] E. LAU, « Principaux enjeux de l'administration électronique dans les pays membres de l'OCDE », *op. cit.*, p. 229.

[674] « L'administration électronique au niveau des pouvoirs fédéral, provincial et local », Rapport fait au nom de la Commission de l'intérieur et des affaires administratives par Mmes Thijs et Van Riet, *Doc. Parl.* Sénat, sess. 2000-2001, n° -2-564/1, p. 5.

[675] SLCE, avis du 2 février 1998 relatif à un avant-projet de loi « transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *op. cit.,* p. 193.

C'est l'objet du premier point. Ces réflexions nous amènent, dans un deuxième temps, à encourager le développement d'un modèle d'e-gouvernement en réseaux.

I. Les impératifs

158.- Privacy by design et circulation des données. La protection de la vie privée doit recevoir une attention particulière dès la mise en place l'e-gouvernement. Cette idée se rattache au concept de *Privacy by design*. Quant à l'efficacité administrative, elle conduit à promouvoir la circulation des données dans l'administration, pour les raisons que l'on développe ci-après.

A. La protection de la vie privée et le concept de Privacy by design

159.- Considérations générales. Il a déjà été longuement question des raisons pour lesquelles il importe de protéger la vie privée des citoyens dans l'e-gouvernement[676]. En revanche, nous n'avons pas encore souligné l'importance de tenir compte des règles de protection de la vie privée dès la mise en place des outils de traitement. Cette méthode s'appelle le *Privacy by design,* que l'on traduit par « respect de la vie privée dès la conception ».

160.- Le concept de Privacy by design. Le concept de *Privacy by design*[677] émerge du constat que, bien souvent, les instruments législatifs ne sont pas suffisants pour encadrer correctement la protection de la vie privée à l'égard des traitements de données à caractère personnel. C'est d'ailleurs ce que nous avons également observé dans notre étude de l'e-gouvernement belge[678]. Bien que des règles existent, elles sont difficilement respectées[679] ou s'avèrent mal adaptées à l'e-gouvernement[680].

---

[676] Voy. *supra,* n°s 59.- et s.

[677] Cette idée a été développée dans les années nonante par Ann Cavoukian, commissaire à la protection de la vie privée de l'Ontario, au Canada, qui y consacre un site internet (www.privacybydesign.ca). Voy. A. CAVOUKIAN, *Privacy by design… take the Challenge,* s.l., 2009.

[678] Voy. *supra,* n°s 79.- et s.

[679] On a montré, par exemple, que le législateur éprouve des difficultés à définir rigoureusement la finalité d'un traitement de données.

[680] Par exemple, l'utilisation très large, au sein de l'administration, du numéro d'identification du Registre national renferme des dangers d'interconnexions illicites, bien que cette utilisation soit encadrée par la loi sur le Registre national.

Privacy by design désigne la méthode qui consiste à intégrer la protection de la vie privée en amont, dans la conception-même du système informatique, plutôt que de créer ce système et de penser seulement ensuite à protéger la vie privée par des normes[681]. Pour le dire autrement, il s'agit de créer des outils qui, en eux-mêmes, présentent des garanties de protection pour la vie privée des personnes concernées. De cette manière, la protection de la vie privée est soutenue par la technique, en sus d'être organisée par des normes. Ensemble, ils constituent « un rempart efficace contre les excès rendus possibles par le progrès »[682].

Le concept de *Privacy by design* reçoit de plus en plus d'importance dans le régime de la protection de la vie privée et des données à caractère personnel. En 2010, elle a fait l'objet d'une résolution adoptée par les commissaires à la protection des données et de la vie privée[683]. Cette résolution définit la notion de *Privacy by design* comme « the philosophy and approach of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle »[684].

Depuis lors, le concept de *Privacy by design* est intégré dans le projet de règlement sur la protection des données[685].

> Ainsi, l'article 23.1 affirme que « le responsable du traitement applique, tant lors de la définition des moyens de traitement que lors du traitement proprement dit, les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée ».

Elle a dès lors vocation à devenir une exigence contraignante pour tous les responsables de traitements, qui devront mettre en œuvre des mesures

---

681 Voy. A. Cavoukian, *op. cit.,* p. 3 ; R. Duaso Cales, *op. cit.,* pp. 300 à 304 ; J. Le Clainche, « Consentement et traitements de données à caractère personnel », *in Les technologies de l'information au service des droits : opportunités, défis, limites* (dir. D. Le Métayer), Bruxelles, Bruylant, 2010, pp. 166 à 169 ; M. Groothuis, « De digitale overheid en de menselijke maat », *Computerrecht,* 2009, p. 240.

682 J. Le Clainche, *op. cit.,* p. 168.

683 Resolution on Privacy by design, 32nd International Conference on Data protection and Privacy Commissioners, Jerusalem 27-29 octobre 2010.

684 *Ibid.*, p. 2.

685 À ce sujet, voy. T. Van Canneyt, « Naar meer efficiënte bescherming van persoonsgegevens – een beknopte bespreking van het voorstel voor een verordening van de Europese commissie », *Cah. Jur.,* 2012/2, p. 57 ; C. Glayrel et R. Robert, « Proposition de règlement sur la protection des données – premiers commentaires », *J.T.*, 2012, p. 176.

techniques garantissant, en amont, le respect des règles de protection des données.

161.- Privacy by design et e-gouvernement belge. Tout en percevant l'importance du *Privacy by design,* on devine que la mise en œuvre de cette méthode n'est pas chose aisée car elle mêle la technique et le droit[686]. La concrétisation de cette idée suppose donc la complicité d'informaticiens et de juristes qui, jusqu'à présent, n'ont malheureusement pas encore eu beaucoup d'occasions de créer un langage de travail commun…

Quoi qu'il en soit, dans le cadre de cette recherche, nous ne prétendons pas proposer un modèle d'e-gouvernement qui réponde parfaitement à l'ensemble des implications techniques et juridiques du concept de *Privacy by design.* Bien plus modestement, notre propos entend montrer que certains outils de traitements dont il a été question précédemment constituent des pistes intéressantes pour organiser un e-gouvernement dans l'esprit du *Privacy by design.* La section suivante en témoigne.

À cet égard, comme on l'a déjà dit[687], la plateforme d'échanges d'informations et la source authentique de données peuvent être des outils offrant, en eux-mêmes, des garanties techniques pour protéger la vie privée des citoyens, à la condition, bien sûr, d'être organisés dans le respect des règles constitutionnelles et des règles de protection des données.

B. L'efficacité administrative et la circulation des données

162.- Encourager la circulation des données. Le deuxième impératif dont il faut tenir compte dans la confection d'un modèle d'e-gouvernement est celui de l'efficacité administrative. Pour l'heure, les textes réglementant l'usage des données à caractère personnel sont principalement fondés sur une « conception traditionnelle d'une protection des données unilatérale, à caractère purement défensif »[688]. Ils visent surtout à contenir « les velléités de surveillance de l'administration »[689] et, de ce fait, à prohiber les échanges de données[690].

---

[686] J. Verdure, « Le concept de « Privacy by Design » : un remède à l'insuffisance des moyensactuels de protection de la vie privée », février 2012, article publié sur le site http://www.e-juriste.org

[687] Voy. *supra,* n° 146.-

[688] T. Würtenberger et G. Sydow, *op. cit.,* pp. 368-369.

[689] P. Trudel, « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », *op. cit.,* p. 258.

[690] Voy. égal. T. Würtenberger et G. Sydow, « Administration électronique et protection de la vie privée en Allemagne », *in L'administration électronique au service des citoyens* (dir. G. Chatillon et B. du Marais), Bruxelles, Bruylant, 2003 ; R. Duaso Calès, *op. cit.,* pp. 43 et 44.

Ces barrières freinent inutilement l'efficacité administrative. La protection des données peut être assurée autrement dans l'administration, en encourageant la circulation des données tout en l'encadrant suffisamment. En d'autres termes, organiser, au sein de l'administration, une circulation des données correctement balisée paraît être une solution plus protectrice des droits citoyens qu'entretenir la méfiance face à de tels échanges. En effet, la méfiance aboutit à interdire des échanges ou à les autoriser à partir de motifs souvent peu compréhensibles[691]. On le déplore actuellement en constatant que cette attitude aboutit à un e-gouvernement peu homogène, dans lequel il est difficile de savoir quelle autorité détient quelles données et ce qu'elle en fait. La prévisibilité des traitements de données et le contrôle de ceux-ci s'en trouvent affectés. Comme l'affirme Pierre Trudel, dans l'e-gouvernement, « les internautes, citoyens, gestionnaires et agents de l'État sont en mesure de communiquer, partager, et échanger des informations. Compte tenu de ce contexte, le cadre juridique relatif à l'information qui est nécessairement en possession de l'Administration, devrait s'attacher à en régir les conditions d'accès par chaque agent de l'État plutôt que d'en interdire la circulation. Dans un État en réseau, l'enjeu n'est plus tellement de savoir si une information peut ou non être en possession de l'Administration mais plutôt si cette dernière a le droit d'y accéder et d'en faire usage pour prendre une décision dans une situation spécifique »[692].

À cet égard, la volonté du législateur belge d'ancrer, dans l'administration, le principe de la collecte unique des données est à encourager. L'élaboration d'un modèle d'e-gouvernement belge doit concrétiser cette ambition de manière harmonieuse.

Plusieurs raisons convainquent d'étendre le principe de la collecte unique des données à l'ensemble de l'administration. Elles tiennent tant à la satisfaction d'exigences de protection des données qu'au respect de règles de droit administratif.

---

[691] En ce sens, P. Trudel, « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *op. cit.*, p. 250 ; du même auteur, « The Development of Canadian Law with espect to E-government », *op. cit.,* pp. 124 et 125 ainsi que pp. 132 à 135 ; T. Würtenberger et G. Sydow, *op. cit.,* pp. 368-370.

[692] P. Trudel, « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *Revista catalana de dret public,* 2007, p. 250. Voy. égal. du même auteur, « The Development of Canadian Law with espect to E-government », *in* J.E.J. Prins (dir.), *Designing e-Government,* The Hague, Kluwer Law International, 2007, pp. 124 et 125 ainsi que pp. 132 à 135. Dans le meme sens, R. Duaso Calès, *op. cit.,* pp. 51 à 62.

§1. Les raisons liées à la protection des données

163.- La qualité des données. Rappelons[693] que la collecte unique des données a pour corollaire l'obligation de collecte indirecte des données. Si les informations ont déjà été demandées au citoyen et qu'elles sont disponibles dans le réseau, l'administration qui en a besoin ne peut en principe plus les demander à la personne concernée. Elle doit s'adresser à l'administration qui les détient.

En soumettant les administrations à l'obligation de collecte indirecte des données, on organise la circulation des informations au sein de l'administration. Ce faisant, on répond à une exigence importante du régime juridique de la protection des données, celle de la qualité des données. En effet, l'obligation de collecte indirecte des données garantit que seules des données exactes et à jour seront utilisées. Puisque les administrations ne doivent plus chacune s'adresser aux personnes concernées et veiller ensuite à la mise à jour des données collectées, on supprime les risques que des erreurs soient commises dans l'encodage des données et dans leur actualisation[694].

164.- La proportionnalité des données et la finalité du traitement. La circulation des données dans l'e-gouvernement doit être rendue techniquement possible par la mise en place d'une plateforme d'échanges de données qui, placée au cœur du réseau sectoriel, est chargée de transférer les données d'une administration à l'autre[695]. On doit également penser à impliquer davantage les détachés à la protection des données, qui sont des spécialistes de la protection des données œuvrant au sein de chaque administration[696].

Si ces mesures sont mises en place par le législateur, comme on l'encourage à le faire dans les développements qui suivent[697], la circulation des données au sein de l'administration permet également de veiller à ce que les administrations impliquées dans un échange de données respectent les exigences de proportionnalité des données, et de finalité du traitement. En effet, les détachés à la protection des données des administrations qui envisagent d'effectuer un transfert de données seraient chargés de vérifier la légalité d'un tel transfert, en veillant à ce que seules les données

[693] Voy. *supra*, n° 9.-

[694] Cela suppose bien évidemment que la donnée collectée et enregistrée dans la source authentique de données soit exacte. L'exactitude de la donnée doit être garantie par l'administration responsable de la source authentique de données. Voy. *supra*, n°s 139.- et s.

[695] À ce sujet voy. *supra*, n° 20.- et n°s 139.- et s.

[696] Au sujet des détachés à la protection des données, voy. *infra*, n°s 552.- et s.

[697] Voy. *infra,* n°s 172.- et s.

pertinentes soient communiquées et qu'une finalité déterminée, explicite et légitime justifie un tel traitement de données. Ensuite, la plateforme d'échanges pourrait vérifier également que ces conditions sont respectées au moment du transfert effectif des données.

§2. Les raisons liées au droit administratif

165.- L'allègement des obligations de collaboration et la satisfaction de principes généraux de bonne administration. La collecte unique des données et l'obligation de collecte indirecte imposée aux administrations répond également à des impératifs qui émanent du droit administratif.

Plus particulièrement, la circulation des données allège certaines obligations légales qui pèsent sur le citoyen, que l'on qualifie ici d'obligations légales de collaboration. La collecte indirecte des données permet d'alléger ces obligations et, dès lors, d'aider le citoyen à les respecter plus aisément.

La circulation des données répond également à certaines préoccupations du droit administratif, consacrées par des principes de bonne administration, c'est-à dire, des « règles dont l'application aux autorités administratives doit permettre à celles-ci d'agir de façon prudente, raisonnable et soigneuse, particulièrement dans leurs relations avec les citoyens »[698].

Ainsi, le droit administratif veille à ce que les agents de l'administration accomplissent leur mission avec minutie. Grâce à la collecte indirecte des données, les tâches administratives peuvent être accomplies avec plus de minutie encore.

Par ailleurs, les décisions administratives doivent être prises dans un délai raisonnable. À cet égard également, la collecte indirecte de données offre des facilités certaines pour satisfaire à ce principe de bonne administration.

1. Un allègement des obligations légales de collaboration

166.- Les obligations légales de collaboration. Certaines lois imposent au citoyen de fournir tous les documents utiles à l'examen de la demande qu'il a introduite auprès d'une administration. Si le citoyen se montre négligent, il sera déchu du droit qu'il réclamait à l'autorité administrative,

[698] J.-F. Neven et D. De Roy, « Principes de bonne administration et resopnsabilités de l'O.N.S.S. », *in La sécurité sociale des travailleurs salariés. Assujettissement, cotisations et sanctions*. (dir. J.-F. Neven et S. Gilson), Bruxelles, Larcier, 2010, p. 510. Voy. égal. F. Bundshuch-Rieseneder, « Governance and e-governance in the frame of Bologna Process », *in Bologna Process, European Construction, European Neighbourhood Policy* (T. Come et G. Rouet), Bruxelles, Bruylant, 2011, pp. 254 et 255.

« ce qui permettra à [celle-ci] de prendre ou de maintenir une décision qui va à l'encontre d'un droit subjectif que le citoyen pensait pouvoir réclamer ou qui ne permettra plus au citoyen de réclamer une certaine action ou abstention de la part de l'autorité »[699]. Ce type d'obligation s'impose notamment dans les relations entre les citoyens et les institutions de sécurité sociale.

> Par exemple, s'agissant du droit à l'intégration sociale, la loi du 26 mai 2002 dispose que « l'intéressé est tenu de fournir tout renseignement et autorisation utile à l'examen de sa demande »[700].
>
> Autre exemple. En matière de droit à la pension dans le secteur public, l'article 59 de la loi du 24 décembre 1976[701] affirme que « demeurent acquises à ceux qui les ont reçues, les sommes payées indûment à titre de pension par les pouvoirs et organismes cités à l'article 58 lorsque le remboursement n'en a pas été réclamé dans un délai de six mois à partir du premier jour du mois au cours duquel le paiement a été effectué. [...]
>
> § 2. (Le délai fixé au § 1er est porté à (trois ans) lorsque les sommes indues ont été obtenues :
>
> [...]
>
> 2° suite à l'abstention par le débiteur d'effectuer la déclaration de changement d'état civil prescrite par une disposition légale ou réglementaire ou résultant d'un engagement souscrit antérieurement ».

167.- L'allègement des obligations légales de collaboration dans l'e-gouvernement. La collecte indirecte de données permet d'alléger les obligations légales de collaboration à deux égards.

D'une part, les charges administratives du citoyen sont réduites : puisque l'administration accède à de nombreuses données personnelles sans les demander à la personne concernée, cette dernière se voit épargnée de multiples formalités administratives.

D'autre part, on ne peut plus sanctionner une personne au motif qu'elle n'a pas fourni elle-même l'information que l'administration exigeait, dans l'hypothèse où la loi organise une obligation de collecte indirecte

---

[699] J. De Staercke, « Le principe de bonne citoyenneté et le principe de chercher bon droit », *C.D.P.K.* 2004, p. 88. Voy. également O. Daurmont et D. Batselé, « 1985-1989 : cinq années de jurisprudence du Conseil d'État relative aux principes généraux du droit administratif », *A.P.T.,* 1990, p. 269, note 69 ; C.E., n° 25.781, 29 octobre 1985, *Bortels*.

[700] Art. 19, §2, de la loi du 26 mai 2002 concernant le droit à l'intégration sociale, *M.B.,* 31 juillet 2002.

[701] Loi relative aux propositions budgétaires 1976-1977, *M.B.,* 28 décembre 1976, depuis sa modification par l'art. 54 de la loi du 3 février 2003 apportant diverses modifications à la législation relative aux pensions du secteur public, *M.B.,* 13 mars 2003.

qui impose à l'administration de trouver, par elle-même, l'information recherchée.

Avant d'étayer davantage le précédent constat, remarquons d'emblée que l'allègement des obligations légales de collaboration n'est pas une faveur que l'administration pourrait consentir, ou non, au citoyen. Pareille simplification administrative est imposée par le principe de la réciprocité des avantages, selon lequel les technologies qui renforcent l'action de l'administration doivent également bénéficier au citoyen. Ce principe a été mis en évidence par Yves Poullet et est repris, depuis lors, par la CPVP[702]. D'autres auteurs de doctrine[703] ainsi que plusieurs directives européennes organisant l'usage de certains outils électroniques en font également application[704].

Le principe de la réciprocité des avantages est développé et justifié dans la suite de la recherche[705]. Signalons déjà que, selon Yves Poullet, il s'agit, pour le législateur de mettre « à charge de celui qui utilise la technologie aux fins de développer ses activités professionnelles, certaines obligations supplémentaires qui permettent de rétablir l'équilibre traditionnel des parties en présence », au motif que « si la technologie accroît les capacités de collecte de traitement, de communication des informations relatives à autrui, si la technologie facilite la conclusion de transactions ou d´opérations administratives, il est indispensable que cette même technologie soit configurée et utilisée de manière telle que la personne concernée, l´administré, le consommateur, bref le fiché, puisse bénéficier, dans une proportion comparable, des avantages de cette technologie »[706].

Ce principe trouve à s'appliquer ici. La collecte indirecte des données facilite l'exécution des tâches de l'administration. En vertu du principe de réciprocité des avantages, il s'impose également de faciliter les tâches administratives du citoyen. Ce faisant, les obligations légales de collaboration qui s'imposent à un citoyen dans ses relations avec l'administration, sont allégées et, de ce fait, plus aisément respectées par tout un chacun.

a) La réduction des charges administratives du citoyen. La collecte indirecte réduit les charges administratives des personnes qui effectuent

---

[702] Voy. CPVP, avis n° 01/2007, *op. cit.,* p. 15, n° 83.

[703] Voy. *infra,* n°s 382.-et s.

[704] Par exemple, la directive 2001/31/CE sur les services à la société de l'information prévoit la possibilité de s'opposer au spamming « via des moyens électroniques ». Pour de plus amples détails à ce sujet, voy. Y. Poullet, « Pour une troisième génération de législation de protection des données », *op. cit.,* p. 11.

[705] Voy. *infra,* n°s 382.- et s.

[706] Y. Poullet, « Pour une troisième génération de réglementation de protection des données », *in Défis du droit à la protection de la vie privée. Perspectives du droit européen et Nord-américain* (dir. M.V. Perez Asinari et P. Palazzi), Bruxelles, Bruylant, 2008, pp. 57 et 58.

une démarche auprès de l'administration[707]. En effet, étant obligée d'obtenir l'information d'une source authentique, l'administration ne doit plus demander au citoyen de la lui fournir.

Cet allègement des obligations légales de collaboration dans de telles hypothèses est aisément compréhensible : l'administration dispose d'outils technologiques performants qui facilitent sa tâche et lui permettent de l'accomplir plus rapidement. Il est juste que le citoyen jouisse également de telles avancées en voyant sa tâche facilitée, ce qui apparaît comme une compensation dans son chef de la performance nouvelle de l'administration. C'est ce qu'on a qualifié plus haut de « principe de réciprocité des avantages ».

b) L'interdiction de sanctionner le citoyen. L'obligation de collecte indirecte entraîne une conséquence importante puisque le citoyen ne pourra être sanctionné du fait de ne pas avoir communiqué une information que l'administration devait obtenir par elle-même. C'est d'ailleurs ce qu'affirment déjà plusieurs lois sectorielles.

> Par exemple, la loi sur la Banque-Carrefour des véhicules et la loi sur la Banque-Carrefour des Entreprises affirment que « les services habilités à consulter les données [enregistrées dans la Banque-Carrefour] ne peuvent plus, si ces données ne leur sont pas communiquées directement, en imputer la faute à ces personnes[708] »[709]. La loi sur le Registre national formule l'interdiction d'une sanction en prévoyant que « dès qu'une donnée a été communiquée au Registre national et enregistrée dans ledit Registre, la personne concernée n'est pas tenue de la communiquer directement aux autorités, organismes et personnes [...] autorisés à consulter les données du Registre national »[710].

Bien que les cas de jurisprudence faisant application de l'obligation de collecte indirecte des données soient rares, deux arrêts très pertinents retiennent notre attention. L'un concerne le calcul du droit à la pension et l'autre, l'octroi du revenu d'intégration social. Ces deux décisions mettent en évidence le fait que la collecte indirecte des données n'est pas un mécanisme dont les administrations peuvent user à leur guise, quand bon leur semble. Les juges rappellent qu'il s'agit d'une contrainte légale

[707] La CPVP l'a elle-même souligné dans son avis n° 49/2006, *op. cit.*, p. 6, n° 33.

[708] Il s'agit des personnes physiques et morales propriétaires d'un véhicule, dans le cas de la Banque-Carrefour des véhicules, et des entreprises et des mandataires de celles-ci, dans le cas de la Banque-Carrefour des entreprises.

[709] Art. 23 de la loi sur la Banque-Carrefour des véhicules, et art. 22 de la loi sur la Banque-Carrefour des entreprises.

[710] Art. 6, §2, de la loi du 8 août 1983.

permettant aux administrations, mais aussi aux personnes dont les données sont traitées, de bénéficier des avantages de l'e-gouvernement.

b-1. Le 27 juin 2006, la Cour du travail de Liège a rendu un arrêt faisant application de l'obligation de collecte indirecte en matière de *droit à la pension*[711]. L'Office national des pensions reprochait à un homme pensionné de ne pas l'avoir averti du décès de son épouse, ce qui avait des conséquences au niveau du montant de la pension qui lui était due. L'Office national des pensions exigeait de récupérer les sommes indûment payées depuis cinq ans, en application du délai de prescription applicable en cas de mauvaise foi de l'assuré social ou lorsque l'indû trouve son origine « dans l'abstention du débiteur de produire une déclaration prescrite par une disposition légale ou réglementaire ou résultant d'un engagement souscrit antérieurement », plutôt que de se soumettre au délai de prescription de six mois en principe applicable[712].

Cet assuré social avait averti la commune du décès de son épouse. Cette information était donc enregistrée au Registre national. Faisant partie du réseau sectoriel de la sécurité sociale, l'Office national des pensions y avait donc accès par l'intermédiaire de la Banque-Carrefour de la sécurité sociale.

Compte tenu de ces éléments de fait et de droit, la Cour affirme qu' « un assuré social ne peut se voir imposer personnellement une obligation qui doit déjà être légalement remplie par une institution dont c'est la mission. C'est donc à tort que l'O.N.P. soutient que l'information transmise par la Banque-Carrefour doit être doublée par une information émanant de l'assuré social et que seule celle-ci permettrait au pensionné de remplir ses obligations envers lui [...] »[713].

b-2. Le 21 avril 2010, la Cour du Travail de Bruxelles[714] a fait droit à la demande d'un assuré social, Monsieur E.G., qui réclamait le *revenu d'intégration sociale*. Le CPAS refusait l'octroi de cette indemnité, au motif que Monsieur E.G. n'avait pas fourni un certain nombre de documents et avait dès lors manqué à son devoir de collaboration.

Dans sa motivation, la Cour du Travail rappelle l'existence de l'article 11 de la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale, qui prévoit que « lorsque les données sont disponibles dans le réseau, les

[711] C. trav. Liège, 27 juin 2006, *J.L.M.B.,* 2007, pp. 1043-1047.

[712] Ces délais sont imposés par l'article 21, §3, de la loi du 13 juin 1966 relative à la pension de retraite et de survie des ouvriers, des employés, des marins naviguant sous pavillon belge, des ouvriers mineurs et des assurés libres.

[713] C. trav. Liège, 27 juin 2006, *op. cit.,* p. 1047.

[714] C. trav. Bruxelles (8e ch.), 21 avril 2010, R.G. n° 2008/AB/51591 et n° 2009/AB/51809.

institutions de sécurité sociale sont tenues de les demander exclusivement à la Banque-Carrefour ». La Cour affirme qu'il faut déduire de cette disposition légale qu' « un manque de collaboration du demandeur ne peut être envisagé à propos d'informations auxquelles le CPAS peut accéder, accessibles via la Banque-Carrefour de la sécurité sociale »[715].

Or, en l'espèce, « la plupart des documents prétendument manquants étaient accessibles via la Banque-Carrefour ou le Registre national : le CPAS n'avait pas à la demander à Monsieur E.G. ; il aurait dû les recueillir d'initiative »[716].

C'est pourquoi, la Cour décide que Monsieur E.G. a droit au revenu d'intégration sociale[717].

D'autres exemples allant dans le même sens peuvent être imaginés. Ainsi, l'ONEm ne pourrait pas refuser à un chômeur l'octroi de son allocation de chômage au motif qu'il n'aurait pas fourni les données nécessaires à l'établissement de son droit. En effet, cette institution est en mesure d'obtenir ces informations grâce à la Banque-Carrefour de la sécurité sociale. Dans le même sens, si le SPF Finances envoie l'avertissement extrait de rôle à l'ancienne adresse d'un contribuable, celui-ci risque de ne pas le recevoir et dès lors, de ne pas payer, dans les délais requis, le montant éventuellement réclamé. Le SPF Finances ne pourrait pas reprocher ce retard au citoyen en le taxant d'office, étant donné qu'il revenait à cette administration de mettre à jour la donnée relative au domicile de ce contribuable en exerçant son droit d'accès au Registre national.

168.- La condition de l'autorisation du comité sectoriel. Soulignons, enfin, que l'interdiction de sanctionner le citoyen ne vaut, évidemment, que si l'administration concernée est effectivement en mesure d'effectuer une collecte indirecte de données. Or, pour l'heure, une administration ne peut, en principe, accéder indirectement à des données que si elle y a été autorisée par un comité sectoriel et ce, même si elle appartient à un réseau sectoriel.

> Par exemple, les institutions de sécurité sociale faisant partie du réseau de la sécurité sociale doivent, en principe, demander l'autorisation du comité sectoriel de la sécurité sociale et de la santé[718].

Deux précisions doivent être apportées à cet égard.

---

715 *Ibid.*, 4e feuillet.

716 *Ibid.*, 6e feuillet.

717 *Ibid.*, 8e feuillet.

718 Art. 15 de la loi sur la Banque-Carrefour de la sécurité sociale. La loi prévoit également que le Roi peut prévoir des exceptions à cette obligation.

Premièrement, l'administration soumise à l'obligation de collecter les données indirectement est obligée de demander l'autorisation du comité sectoriel compétent. En d'autres termes, elle ne pourrait soutenir qu'elle n'est pas autorisée à accéder aux données au motif qu'elle n'a pas demandé cette autorisation. Ainsi, l'obligation de collecte indirecte des données inclut l'obligation de demander l'autorisation d'accéder aux données.

Deuxièmement, il faut souligner que si le comité sectoriel refuse d'autoriser l'administration à collecter indirectement les données, elle ne pourra pas nécessairement effectuer une collecte directe de données auprès des personnes concernées. En effet, tout dépend de la raison pour laquelle le comité sectoriel a refusé l'autorisation. Si le refus est lié à une violation de la loi – soit que les données demandées n'entrent pas dans les missions de l'administration, soit que la collecte ne poursuit pas une finalité déterminée, explicite et légitime ou encore si les informations réclamées sont disproportionnées – l'administration ne pourrait collecter ces informations auprès des personnes concernées. Par contre, si le refus du comité sectoriel est lié à la disproportion du traitement lui-même parce qu'il est électronique, on peut raisonnablement soutenir que l'administration pourrait recourir à une collecte directe. En effet, le comité sectoriel pourrait refuser la collecte indirecte au motif qu'elle est disproportionnée puisqu'elle se fait à l'insu des personnes concernées et qu'un tel transfert porterait sur des données relatives à un grand nombre d'administrés. La collecte directe permettrait d'obtenir les données en informant les personnes concernées une à une.

2. Un renforcement du devoir de minutie

169.- Minutie et informations exactes et à jour. La collecte indirecte des données permet aux administrations d'obtenir facilement et rapidement une information exacte et à jour. En cela, elle apparaît comme une application légale du devoir de minutie, appelé également principe de prudence, qui, rappelons-le, « oblige l'autorité à procéder à une recherche minutieuse des faits, à récolter les renseignements nécessaires à la prise de décision et à prendre en considération tous les éléments du dossier, afin qu'elle puisse prendre sa décision en pleine connaissance de cause et après avoir raisonnablement apprécié tous les éléments utiles à la résolution du cas d'espèce »[719].

En effet, l'administration est souvent amenée à devoir prendre des décisions à partir d'informations dont elle ne dispose pas. Certaines d'entre

[719] J. JAUMOTTE, « Les principes généraux du droit administratif à travers la jurisprudence administrative », *op. cit.*, p. 687 et les références de jurisprudence citées. Voy. égal. O. DAUR-

elles peuvent être difficiles à obtenir de la part du citoyen. Ce dernier a peut-être égaré les documents pertinents, ou n'est pas en mesure d'effectuer les calculs complexes que ces informations exigent[720], etc.

Pourtant, l'administration doit se soumettre à ce devoir de minutie, d'autant plus qu'il s'applique à elle avec une exigence particulière. En effet, l'administration jouit « de caractéristiques, de spécificités et d'expériences particulières »[721] et dispose de moyens d'information dont sont privés les autres sujets de droit[722]. Ces éléments poussent à apprécier son comportement non pas au regard du comportement de tout homme normalement prudent et raisonnable mais bien au regard du comportement d'un professionnel car, « comme tout professionnel – en l'occurrence professionnel du service public –, elle a l'obligation d'agir dans les règles de l'art »[723].

170.- Une appréciation plus rigoureuse de la minutie. En l'état actuel de nos recherches, nous n'avons pas connaissance de cas de jurisprudence interprétant le devoir de minutie au regard des moyens techniques désormais à disposition de l'administration. Néanmoins, on peut raisonnablement penser que la mise en place des outils informatiques puissants qui facilitent l'accès des administrations aux données des citoyens, et qui leur permettent également d'en obtenir régulièrement la mise à jour, sont des éléments dont les juges pourraient tenir compte pour apprécier plus sévèrement encore ce devoir de minutie appliqué à l'administration.

La collecte indirecte de données apparaît donc comme une nouvelle obligation légale aidant l'administration à respecter le devoir de minutie qui s'applique traditionnellement à elle et qui pourrait, à l'avenir, être interprété plus sévèrement compte tenu des facultés techniques dont l'administration dispose désormais.

MONT et D. BATSELÉ, *op. cit.,* p. 267 ; M. PÂQUES, « L'application de la loi fiscale. Principes de bonne administration en droit administratif et en droit fiscal. Présentation et mise en œuvre », *Act. Droit.,* 1993, pp. 422 à 424.

720 Tel est le cas en matière d'allocations familiales, notamment.

721 L. CORNELIS, *Principes de droit belge de la responsabilité extra-contractuelle*, Bruxelles, Bruylant, Anvers, Maklu, 1991, p. 219.

722 Conclusions du Procureur général Dumon précédant un arrêt de la Cour de cassation du 19 décembre 1980, *R.W.,* 1981-1982, col. 1061, cité par M. PÂQUES, « L'application de la loi fiscale. Principes de bonne administration en droit administratif et en droit fiscal. Présentation et mise en œuvre », *op. cit.,* p. 464.

723 J. PUTZEYS, S. GEHLEN, et J. BOURTEMBOURG, « La bonne foi, critère d'appréciation dans l'acte administratif », *in La bonne foi* (dir. S. DAVID-CONSTANT), Éd. du Jeune Barreau de Liège, 1990, p. 403.

3. Une aide pour le respect du délai raisonnable

171.- Obtention rapide de l'information. La collecte indirecte des données permet, en principe[724], aux administrations, d'obtenir une information rapidement. En cela, cette obligation légale aide l'administration à se prononcer dans un délai raisonnable.

La consultation des sources authentiques de données, les flux de données et de mises à jour de celles-ci générés par les plateformes d'échanges d'informations, sont autant d'éléments qui facilitent la tâche de l'administration et lui permettent d'obtenir rapidement les données dont elle a besoin, sans être tributaire du temps que le citoyen mettra à répondre à sa demande ou à rectifier une réponse inexacte ou incomplète. Comme en ce qui concerne le devoir de minutie, la collecte indirecte de données représente donc une méthode aidant l'administration à respecter cette exigence.

II. Le choix du modèle de l'État en réseaux

172.- Description sommaire du modèle. Compte tenu des avantages qu'offrent le principe de la collecte unique des données et l'obligation corollaire de collecte indirecte des informations, le cadre juridique de l'e-gouvernement doit assurer la disponibilité et la fiabilité des données[725].

Néanmoins, cette circulation des données ne peut être organisée sans balise. Il convient d'appliquer la méthode du *Privacy by design*, afin de mettre en place des outils qui, tout en permettant la circulation des données, contiennent, en eux-mêmes, des garanties pour la protection de la vie privée des citoyens.

Le modèle de l'« État en réseaux »[726] permet une circulation des données respectueuse des impératifs de protection de la vie privée et des données à

---

[724] Pour l'heure, l'obligation de demander l'autorisation du comité sectoriel compétent pour obtenir l'information recherchée est de nature à alourdir la tâche des administrations. C'est pourquoi, nous proposons une solution qui se passe des comités sectoriels. Voy. *infra*, n°s 596.- et s.

[725] T. WÜRTENBERGER et G. SYDOW, *op. cit.*, p. 369.

[726] Ce modèle s'apparente en grande partie au modèle de l' « État en réseau » défendu par le professeur Pierre Trudel, de l'Université de Montréal (voy. not. P. TRUDEL, « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *Revista catalana de dret public,* 2007, pp. 247 à 280 ; « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », *op.cit.,* pp. 257 à 266 ; « Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau », *op. cit.,* pp. 1 à 52 ; « Existe-t-il un droit public de la gouvernance en ligne ? », *in Droit de l'administration électronique. De nouveaux droits pour les usagers. Des nouvelles règles pour les agents* (dir. G. CHATILLON), Bruxelles,

caractère personnel. Il semble répondre à nos préoccupations. Ce modèle est décrit brièvement à ce stade, pour éclairer les réflexions ultérieures qui approfondissent la manière d'organiser l'administration en réseaux.

Ainsi, il s'agit de créer, au sein de l'administration, des réseaux sectoriels. Ces réseaux sectoriels regroupent chacun un certain nombre de sources authentiques et contiendrait, en son cœur, une plateforme d'échange de données. Les données contenues dans ces sources authentiques circulent dans le réseau grâce à un numéro d'identification sectoriel.

Ces aspects du modèle de l'État en réseaux font l'objet d'amples développements dans la troisième section de ce chapitre.

173.- Quelques outils. L'administration belge recourt déjà à quelques outils intéressants au regard des préoccupations qui viennent d'être évoquées. On pense notamment à deux réseaux sectoriels déjà fonctionnels : celui de la santé, via la plateforme *eHealth*, et celui de la sécurité sociale, via la plateforme Banque-Carrefour de la sécurité sociale. D'autres réseaux devraient être développés à l'avenir, notamment dans le domaine administratif traitant des questions liées aux véhicules, grâce à la Banque-Carrefour des véhicules.

Par ailleurs, certaines normes œuvrent à l'élaboration de pareil modèle pour l'e-gouvernement, telles que le décret flamand du 18 juillet 2008 relatif à l'échange de données entre les administrations flamandes qui prévoit la mise en place de sources authentiques et d'une plateforme d'échanges. Il en va de même de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, en vertu duquel le SPF Fedict est une plateforme d'échanges d'informations chargée d'assurer la circulation des données entre les administrations fédérales.

Plusieurs sources authentiques sont déjà en place, telles que le Registre national et la Banque-Carrefour des entreprises. Il reste à parfaire ces outils, notamment en limitant clairement l'étendue des réseaux sectoriels, et à en développer d'autres dans le respect du droit administratif et du régime juridique de la protection des données.

Ces tâches impliquent la collaboration du législateur fédéral, des législateurs communautaires et régionaux. Par ailleurs, le modèle de l'e-gouvernement doit être organisé par une législation nouvelle et adéquate. C'est ce que précisent les développements qui suivent.

Bruylant, 2011, pp. 315 à 318). Pierre Trudel parle d' « État en réseau », le terme réseau étant utilisé au singulier. Nous préférons parler de réseaux, au pluriel, pour faire apparaître d'emblée l'existence de plusieurs réseaux au sein de l'administration.

Section 2. L'encadrement législatif de l'e-gouvernement

174.- Des règles propres au secteur public. Au terme des développements menés dans les deux premiers chapitres, il nous paraît nécessaire d'adopter des règles de protection des données propres au secteur public.

Pour l'heure, la loi du 8 décembre 1992 ne fait pas de distinction entre les règles applicables au secteur privé et celles applicables au secteur public. À cet égard, la Belgique se distingue d'autres États européens.

> Par exemple, la *Bundesdatenschutzgesetz* allemande comprend une partie consacrée aux traitements de données par les administrations[727]. Celle-ci contient notamment des règles relatives à la collecte et au transfert de données dans le secteur public. Elle organise également les droits que les citoyens peuvent faire valoir vis-à-vis des administrations en ce qui concerne la protection de leurs informations personnelles.
>
> Le législateur espagnol a également adopté des règles particulières pour les traitements de données effectués dans le secteur public[728]. Ainsi, la *Ley Orgánica de Protección de Datos de Carácter Personal de España* contient une partie consacrée aux dispositions sectorielles. Parmi celles-ci, un chapitre est consacré au secteur public, qui reprend des règles relatives à la création des fichiers détenus par le secteur public, la communication de données entre administrations ainsi que des exceptions aux droits des citoyens en matière de protection des données à caractère personnel.

L'idée d'adopter des règles de protection des données propres au secteur public n'est pas neuve. Lors des discussions parlementaires qui ont précédé l'adoption de la loi du 8 décembre 1992, la CPVP a demandé que soient édictées des règles particulières pour le secteur public. Cette demande a été rejetée au motif que « les problèmes soulevés par la protection des données à caractère personnel sont, le plus souvent, semblables, voire identiques, dans les deux secteurs. Les mêmes solutions doivent, par conséquent, y être apportées et la distinction voulue par la Commission de la protection de la vie privée ne se justifie nullement »[729].

À notre sens, cette justification n'est pas tenable. Ainsi qu'on l'a dit, la question de la protection des données à caractère personnel se pose avec une acuité particulière dans le secteur public.

---

[727] Voy. la partie II de la *Bundesdatenschutzgesetz*.

[728] Art. 20 à 24 de la Ley Orgánica de Protección de Datos de Carácter Personal de España du 13 décembre 1993.

[729] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la Commission de la Justice par Mme Merckx-Van Goey, *Doc. Parl.,* Ch. Repr., sess. 1991-1992, n° 413/12, p. 10.

Premièrement, la collecte d'informations par les administrations renforce considérablement la puissance de l'État. En effet, les informations demandées sont nombreuses et touchent à de multiples aspects de la vie des citoyens. Ces derniers ne peuvent refuser de les communiquer, sous peine de ne pas bénéficier de la prestation de service public demandée ou de ne pas accomplir leurs obligations civiques. Par ailleurs, le principe de la collecte unique des données engendre une multiplication des transferts de données entre les administrations, ce qui fait perdre aux individus le contrôle de leurs propres données. Ce constat justifie que des règles précises soient adoptées pour encadrer minutieusement l'usage de cette masse de données par l'État. Comme cela a été affirmé dans les discussions préalables à l'adoption de la loi du 8 décembre 1992, il importe de « montrer clairement les engagements que prend l'État pour tous les fichiers dont il dispose. Il est important que le public sache que vis-à-vis de l'État, il peut être extrêmement exigeant, parce qu'il s'agit de la protection de sa vie personnelle par rapport à une structure étatique puissante »[730].

Deuxièmement, dans l'e-gouvernement, les règles de protection des données doivent être interprétées au regard des règles générales de droit administratif. On a ainsi montré que le principe de spécialité applicable aux administrations impose de vérifier la légalité d'un échange de données tant du côté de l'administration qui émet les données, que du côté de l'administration qui les reçoit. Une précision si importante doit être consacrée explicitement par le législateur. On ne peut se contenter de la reléguer dans quelques avis de la CPVP.

Troisièmement, l'analyse de la jurisprudence de la Cour constitutionnelle et de la section de législation du Conseil d'État a montré que l'exigence de légalité consacrée par l'article 22 de la Constitution est sévère et rigoureuse. Elle impose au législateur de définir lui-même les éléments essentiels des traitements de données. Des règles législatives doivent donc organiser les outils de traitements de données qui permettent le fonctionnement de l'e-gouvernement.

C'est pourquoi, cette partie de la recherche vise à dégager des pistes pour élaborer un cadre juridique adapté à l'e-gouvernement, qui tienne compte des exigences du droit administratif ainsi que du régime juridique de la protection des données à caractère personnel.

Nos réflexions s'articulent en trois temps.

[730] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la Commission de la Justice par M. Vandenberghe, *Doc. Parl.,* Ch. Repr., session extr. 1991-1992, n° 445/2, p. 40.

Dans un premier temps, l'adoption de lois particulières est envisagée pour organiser les plateformes d'échanges d'informations, les sources authentiques de données, et régler l'utilisation des numéros d'identification.

Ensuite, on suggère la confection d'une loi-cadre relative à l'e-gouvernement qui définirait le modèle d'e-gouvernement et les outils de traitements sur lesquels se fonde l'administration, et de réglerait l'échange des données au sein des réseaux sectoriels et entre ceux-ci.

Pour terminer, nos développements se consacrent à la nécessaire collaboration qui doit exister entre les législateurs du pays pour organiser l'e-gouvernement et qui peut prendre la forme d'accords de coopération.

I. Des lois particulières

175.- Une loi particulière pour chaque outil. Les plateformes d'échanges, les sources authentiques de données et les numéros d'identification sont des outils de traitements fondamentaux dans l'e-gouvernement, par lesquels transitent les données personnelles des citoyens. On a souligné que ces outils font actuellement l'objet d'une réglementation peu cohérente.

Le législateur doit remédier à ces difficultés. Conformément à la jurisprudence de la Cour européenne des droits de l'homme et de la Cour constitutionnelle étudiée dans le premier chapitre[731], il lui revient de définir les éléments essentiels de ces outils de traitements de données. Dans cette tâche, une attention particulière doit être accordée à la finalité de l'outil, et à sa proportionnalité, pour deux raisons.

D'une part, ce sont deux éléments essentiels des traitements de données qui doivent être définis par le législateur lui-même, comme nous venons de le rappeler. D'autre part, ces deux éléments sont également des exigences cardinales du régime juridique de la protection des données, comme en atteste le deuxième chapitre. Ces deux exigences doivent fonder la détermination, par le législateur, des autres éléments essentiels de ces traitements[732].

[731] Voy. *supra,* n° 103.-

[732] Comme l'a montré le premier chapitre, la finalité et la proportionnalité ne sont pas les seuls éléments essentiels de ces outils de traitements de données à devoir être définis par le législateur. Certains de ces éléments seront abordés dans ce chapitre au travers des exigences de finalité et de proportionnalité, telles que les données de la source authentique de données. D'autres ne le seront pas. On pense notamment au responsable du traitement. Néanmoins, ces aspects ont été définis dans le Prélude et dans le premier chapitre. Au-delà

> Par exemple, en fonction de la finalité de la source authentique de données, le législateur peut définir les données qui seront enregistrées dans cette base de données ; en fonction de la proportionnalité d'un réseau sectoriel, le législateur doit limiter les administrations appartenant à ce réseau.

Par ailleurs, il nous semble judicieux que le législateur adopte une loi particulière pour chaque source authentique de données, chaque plateforme d'échanges d'information et chaque numéro d'identification utilisé dans l'administration. Ces outils sont particulièrement importants dans l'e-gouvernement puisqu'ils se trouvent à la base de chaque traitement de données réalisé. Il convient donc d'être particulièrement attentif à la clarté et la précision des règles qui les encadrent, de manière à ce que chaque citoyen puisse connaître et comprendre le contenu et le fonctionnement de ces outils.

En ce sens, Dag Wiese Schartum affirme que « there are, in my view, strong reasons to pass specialised data protection legislation within specific and important fields. It is key is to identify particularly powerful types of data processing, especially those geared towards supplying various decision-making processes with personal data »[733]. Et d'ajouter que « data protection legislation should descend from its lofty, sovereign solitude and increasingly be made part of various pieces of specialised legislation. Positive effects should be expected, as specialised legislation provides a concrete context that makes regulation easier to understand, and because knowledge of data protection regulation will often improve amongst those primarily affected by it, when its provisions become part of "their" act »[734].

Les développements qui suivent portent sur l'organisation, par le législateur, des plateformes d'échanges d'informations, des sources authentiques de données et des numéros d'identification. Ils se fondent sur l'exigence de légalité et de l'exigence de proportionnalité appliquées à chacun de ces outils. Ainsi qu'on vient de le rappeler, la finalité et la proportionnalité guident le législateur dans la définition des éléments essentiels des traitements de données mis en place au sein de l'administration.

---

de ces développements, ils gagnent à être étudiés au cas par cas, ce qui n'est pas l'objet de la présente thèse qui entend formuler des réflexions de recherche fondamentale, applicables à tout traitement de données.

[733] D.W. Schartum, « Designing and Formulating Data Protection Laws », *International Journal of Law and Technology,* 2008, vol. 18, p. 14.

[734] *Ibid.,* p. 18.

A. Les plateformes d'échanges d'informations

176.- Considérations générales. On l'a dit, une plateforme d'échanges d'informations est un outil de traitement de données qui organise l'échange des informations entre les sources authentiques du réseau sectoriel.

Comme l'impose l'article 22 de la Constitution tel qu'interprété par la Cour constitutionnelle, il revient au législateur de déterminer la finalité de la plateforme d'échanges et de veiller à la proportionnalité de celle-ci. Ce faisant, cet outil devrait permettre les échanges d'informations entre les administrations tout en respectant la protection de la vie privée.

§1. La finalité de la plateforme d'échanges d'informations

177.- Finalité-mère. La plateforme d'échange doit poursuivre une « finalité-mère » à laquelle correspond une grappe d'administrations poursuivant des finalités précises appartenant à la même famille, ou, en d'autres termes, des missions complémentaires par rapport à un même objectif.

Cela revient à dégager, au sein de l'administration, des « familles délimitées de prestations »[735], ou encore des « secteurs d'activité de l'administration »[736]. Ces différents ensembles d'administrations sont désignés par des vocables divers qui représentent la même réalité.

Ainsi, Pierre Trudel utilise le concept d' « aire de partage »[737] ou de « domaine de confiance »[738]. Herbert Burkert parle de « domaine informationnel cloisonné »[739]. L'OCDE insiste sur l'existence de « groupements axés sur le service client » au sein desquels les organismes publics doivent

[735] P. TRUDEL, « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *op. cit.*, p. 265.

[736] H. BURKERT, « Le jugement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses conséquences », *op. cit.,* p. 12.

[737] P. TRUDEL, « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », *op.cit.,* pp. 263 et s. ; P. TRUDEL, Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *op. cit.,* pp. 267 et s.

[738] P. TRUDEL, « Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau », *op. cit.,* p. 43.

[739] H. BURKERT, « Le jugement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses conséquences », *op. cit.,* p. 12.

collaborer[740], tandis que la CPVP et le législateur parlent plus volontiers de « secteur »[741] ou de « réseau »[742].

1. La détermination de la « finalité-mère » d'un réseau sectoriel

178.- Confiance et clarté. La détermination de la « finalité-mère » d'un réseau sectoriel est une question délicate. Pour la résoudre, il n'est pas inutile de se remémorer l'intérêt de tenir compte des prévisions raisonnables des intéressés[743]. En effet, l'e-gouvernement ne peut se développer sans la confiance des citoyens, qui est tributaire du fait que ces derniers ne doivent pas être surpris par certains traitements et encore moins se sentir piégés. En outre, l'exigence de légalité prescrite par l'article 22 de la Constitution suppose que les citoyens comprennent la manière dont les réseaux sont créés. Ils doivent y voir clair.

179.- Les attentes de l'usager. Compte tenu de ces impératifs, il serait judicieux de définir la « finalité-mère » d'un réseau sectoriel en fonction des attentes de l'usager et non des structures gouvernementales actuelles[744], de manière à ce qu'elle soit mieux comprise. Il a d'ailleurs été constaté que la plupart des pays-membres de l'OCDE « s'accordent actuellement pour reconnaître que les services devraient être organisés et fournis en fonction des besoins et des préférences des clients et non selon la logique (ou l'absence de logique) interne des administrations publiques »[745]. C'est aussi la volonté affirmée par plusieurs parlementaires il y a quelques années, qui ont soutenu la nécessité de redessiner l'administration « en fonction des modèles de pensée (intentions) des citoyens et des entreprises »[746].

---

[740] OCDE, « L'administration électronique : un impératif. Principales conclusions », *L'Observateur OCDE,* mars 2004, p. 3, disponible sur le site http://www.observateurocde.org

[741] Entre autres nombreux exemples, voy. CPVP, avis n° 43/2006 du 8 novembre 2006 concernant une demande d'avis du Ministre de l'Emploi et de l'Informatisation relatif à un projet de loi portant dispositions diverses – création d'un comité sectoriel de la sécurité sociales et de la santé, p. 5.

[742] Voy. not. CPVP, avis n° 13/99 précité ; loi du 19 mai 2010 portant création de la Banque-Carrefour des Véhicules, *M.B,* 28 juin 2010. Le terme « réseau » est utilisé dans le cadre de cette analyse.

[743] Voy. *supra*, n° 124.-

[744] P. Trudel, « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *op. cit.,* p. 265.

[745] E. Lau, *op. cit.*, p. 229.

[746] « L'administration électronique au niveau des pouvoirs fédéral, provincial et local », Rapport fait au nom de la Commission de l'intérieur et des affaires administratives par Mmes Thijs et Van Riet, *Doc. Parl.* Sénat, sess. 2000-2001, n° -2-564/1, p. 5.

Toute la difficulté est d'évaluer justement les attentes des citoyens. Pour l'heure, on peut raisonnablement présumer que ceux-ci envisagent l'administration comme une addition de services intervenant dans les aspects administratifs de leur vie de tous les jours. Ils souhaitent que les administrations concernées par chaque problématique administrative fassent le nécessaire pour répondre à leurs demandes mais ils ne se préoccupent pas de savoir concrètement quelle administration fait quoi et à quel stade.

À partir de là, on pourrait dresser la liste des événements de vie des citoyens qui impliquent des démarches administratives. On pense à la naissance, les études, le mariage, le logement, …[747].

On pourrait ensuite regrouper ces événements au sein d'ensembles correspondant aux différentes lignes de vie des citoyens : la santé, les taxes et impôts, la famille, l'emploi, etc. Ces « lignes de vie » correspondraient à la finalité-mère de chaque réseau sectoriel.

Il conviendrait, enfin, de limiter l'étendue des réseaux aux administrations poursuivant des missions complémentaire par rapport à cette finalité-mère, de manière à ne pas surprendre le citoyen, ce qui serait le cas si on prévoyait l'échange de données entre des administrations n'étant pas concernées par les mêmes facettes de vie.

> Cette démarche semble déjà appliquée dans certains États. Ainsi, aux Pays-Bas, les 13 « *Basisregistraties* » de l'administration sont fondés sur cette logique. Ils sont construits en fonction du mode de vie de la plupart des individus : une personne a un travail, une maison, vit à une certaine adresse, localisée sur une parcelle cadastrale, etc.[748], ce qui donne lieu au registre des revenus, des bâtiments et des adresses, au registre du Cadastre etc.
>
> En France, le site www.service-public.fr renseigne aux citoyens l'existence de « grands fichiers nationaux » en renvoyant au site internet de la CNIL. Ce dernier contient une page intitulée « fichiers en fiche »[749] classés par thèmes : travail, santé, vie citoyenne, éducation, transports, etc.[750].
>
> En Belgique, cette démarche est utilisée pour améliorer la structure des portails internet des administrations, dans le cadre de l'amélioration du *front-office*. On pourrait imaginer transposer cette structure au *back-office* et à la structure des réseaux sectoriels. Ainsi, depuis l'accord de coopération de

[747] *Idem*.

[748] P. VAN DER MOLEN, « Authentic Registers and Good Governance », *op. cit.*, p. 8.

[749] http://www.cnil.fr/en-savoir-plus/fichiers-en-fiche/

[750] Au sujet de l'administration française bâtie autour du citoyen, voy. M.-C. ROQUES-RONNET, « L'e-administration : un progrès pour l'administration publique et pour les citoyens ? », *in Les techniques de l'information au service des droits : opportunités, défis, limites* (dir. D. LE MÉTAYER), Bruxelles, Bruylant, 2010, pp. 248 à 250.

2001[751], l'État fédéral, les Communautés et les Régions se sont accordés sur des « lignes de vie » communes, afin que, quel que soit le portail sur lequel se rend l'utilisateur, il trouve une « structure de présentation de l'information similaire et connue »[752]. Celles-ci sont « avoir un enfant et en prendre soin », « apprendre et se former tout au long de sa vie », « se loger », « travailler », « vie de famille et vie personnelle » etc. À chacune de ces rubriques correspond un ensemble de sous-rubriques[753].

2. Une finalité explicite

180.- Une indication claire. Pour répondre à l'exigence d'une finalité explicite, la finalité-mère doit apparaître clairement dans la loi de manière à cerner les limites du réseau au cœur duquel œuvre la plateforme.

> En ce sens, concernant les plateformes d'échanges de données, la CPVP insiste sur la nécessité de délimiter clairement son champ d'action car il importe d'éviter le « chevauchement des champs d'action » de ces plateformes. En effet, il faut que l' « utilisateur potentiel dispose d'un interlocuteur clair pour un domaine spécifique et qu'une application univoque [...] de la protection de la vie privée soit garantie »[754]. En outre, « il faut exclure le 'shopping' entre les intégrateurs de services. Un tel phénomène serait en effet néfaste à terme pour la sécurité de l'information. Afin de pouvoir économiser sur les dépenses pour la sécurité de l'information par exemple, un utilisateur sera tenté de s'engager avec l'intégrateur qui pose le moins d'exigences à cet égard. Conséquence : un nivellement de la sécurité par le bas plutôt que par le haut »[755].

Malheureusement, l'obligation d'indiquer clairement la finalité de la plateforme d'échanges n'est pas encore respectée en pratique. Il existe

---

751 Accord de coopération du 23 mars 2001 entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire française, et la Commission communautaire commune concernant les principes pour un e-gouvernement intégré et la construction, l'utilisation et la gestion de développements et de services d'un e-gouvernement intégré, *M.B.*, 19 octobre 2006. *Voy. infra*.

752 Easi-wal, « Les lignes de vie », disponible sur le site http://easi.wallonie.be/easi/col_gauche_niveaux_fr/easi-wal/dossiers-thematiques/gestion-du-web/portail-wallonie-be/index.html ?LANG=fr.

753 Voy. le site de Easi-Wal, http://easi.wallonie.be/easi/col_gauche_niveaux_fr/easi-wal/dossiers-thematiques/gestion-du-web/portail-wallonie-be/index.html ?LANG=fr.

754 CPVP, recommandation n° 03/2009, *op. cit.,* p. 7, n° 22.

755 CPVP, avis n° 41/2008 du 17 décembre 2008 concernant l'avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de Services fédéral, p. 5, n° 14 ; CPVP, recommandation n° 03/2009, *op. cit.,* p. 10, n° 34.

actuellement deux réseaux sectoriels dans l'administration belge. Il s'agit de la santé, au sein duquel les échanges de données sont organisés par la plateforme *eHealth*, et de la sécurité sociale, au sein duquel les échanges de données sont organisés par la plateforme Banque-Carrefour de la sécurité sociale. D'autres réseaux devraient être développés à l'avenir, notamment dans le domaine des véhicules, grâce à la Banque-Carrefour des véhicules.

On regrette le flou dont est empreinte tant la finalité de la Banque-Carrefour de la sécurité sociale que celle de la plateforme *eHealth.* En effet, la loi sur la Banque-Carrefour de la sécurité sociale prévoit que la Banque-Carrefour accomplit certaines missions au bénéfice des « institutions de sécurité sociales », définies, en somme, comme les institutions ou les personnes appliquant la sécurité sociale. La difficulté majeure réside dans le fait que la notion de sécurité sociale, définie par la loi, peut être modifiée par le Roi[756]. En outre, la loi habilite le Roi à étendre le réseau « à d'autres personnes que les institutions de sécurité sociale »[757]. De telles habilitations complexifient tant l'identification des administrations intégrées dans le réseau de la sécurité sociale qu'on doute de leur constitutionnalité au regard de l'article 22 de la Constitution. Dans le même sens, on déplore que la délimitation du réseau sectoriel de la santé repose sur les termes « soins de santé », trop généraux pour qu'un citoyen puisse comprendre quelles administrations fournissent et reçoivent des donnés via la plateforme *eHealth.*

181.- Intégrateur de services. La plateforme d'échanges d'informations peut également être un intégrateur de service, et assumer des services autres que le seul échange de données entre les administrations du réseau. Dans ce cas, la finalité doit être complétée en conséquence. En effet, l'intégration de services « doit être considérée comme une finalité distincte et pas simplement la dérivée d'une autre finalité »[758]. Dès lors, la loi doit indiquer que la plateforme d'échanges est également un intégrateur de services et identifier les services ainsi que les administrations auxquels ces services s'adressent. Il peut s'agir, par exemple, de l'anonymisation des informations lorsqu'elles transitent par l'intégrateur avant de les communiquer à l'administration demanderesse des données.

[756] Art. 1, dernier al., de la loi du 15 janvier 1990 précitée.
[757] Art. 18 de la loi du 15 janvier 1990 précitée.
[758] CPVP, recommandation n° 03/2009, *op. cit.,* p. 6, n° 18.

3. Le répertoire des références

182.- Un document à encadrer. La plateforme d'échanges d'informations, éventuellement intégrateur de services également, peut reposer sur un répertoire des références[759].

Bien qu'il ne reprenne pas les données dites « de contenu », ce répertoire contient l'indication de l'emplacement des données à caractère personnel des individus au sein du réseau. Dès lors, il donne un aperçu du profil du citoyen.

> Par exemple, de la référence « ONAFTS- code qualité 102 », on peut déduire que la personne concernée est un travailleur salarié, qui a au moins un enfant et que les allocations familiales lui sont payées en priorité. On peut également présumer qu'il s'agit d'une femme étant donné qu'en principe, les allocations familiales sont payées en priorité à la mère.

Un citoyen peut légitimement craindre l'utilisation qui sera faite d'un tel document. Dès lors, il importe, selon nous, que le législateur indique l'existence d'un répertoire de référence auprès de la plateforme. Il doit également en détailler le contenu, en mentionnant les tables qui le composent : le répertoire des personnes (table « qui-où-quand-en quelle qualité »), la table des données disponibles (« quoi-où »), la table des autorisations d'accès (« qui-peut obtenir-quoi »)[760]. Il doit, enfin, préciser la finalité de chacune de ces tables.

§2. La proportionnalité de la plateforme d'échange de données

183.- Etendue du réseau et détermination des fournisseurs et des destinataires. Le législateur doit déterminer le réseau encadrant la plateforme d'échanges de données en veillant, d'une part, à ce que le réseau ne soit pas trop étendu et, d'autre part, à ce que les fournisseurs et les destinataires des données soient mentionnés dans la loi.

1. Un réseau limité

184.- Un nombre limité d'institutions participatives. Le réseau sectoriel entourant la plateforme d'échanges ne peut être trop étendu. Il importe de limiter les institutions entre lesquelles les données vont être échangées et ce, pour plusieurs raisons.

---

[759] Voy. *supra* n°s 19.- et s.

[760] CPVP, recommandation n° 03/2009, *op. cit.,* p. 7, n° 25.

Tout d'abord, au sein d'un réseau, le contrôle de l'échange des données est assoupli[761]. Pour éviter des abus dans l'utilisation des données, nuisibles à la protection des données des citoyens, il convient de limiter le réseau sectoriel à des administrations ayant des missions apparentées. Il importe en effet de garantir qu'au sein des réseaux, « les renseignements personnels ne seront utilisés qu'à des fins apparentées et compatibles avec celles de la collecte initiale »[762].

Ensuite, pour satisfaire à l'exigence de prévisibilité de la loi requise par l'article 22 de la Constitution, les citoyens et les administrations doivent pouvoir aisément identifier les administrations appartenant au réseau. Un champ d'action trop étendu mettrait en péril le respect de cet impératif. La CPVP a insisté sur ce point, soulignant qu'il est crucial que les champs d'action des plateformes ne se chevauchent pas afin que la plateforme compétente et les règles à suivre apparaissent clairement[763], « tant pour les utilisateurs que les non-initiés »[764].

Enfin, les échanges effectués au sein du réseau doivent pouvoir être contrôlés, pour assurer l'effectivité des règles de protection des données. Cela suppose notamment que le parcours des données puissent être retracé sans trop de difficulté, ce que l'on peut davantage garantir dans un réseau de portée limitée[765].

Si de telles précautions n'étaient pas prises, il y aurait un déséquilibre entre l'efficacité administrative – qui serait garantie – et la protection de la vie privée des citoyens – fortement menacée. Dans un tel contexte, la proportionnalité de l'outil de traitement ne serait pas assurée.

185.- Critiques concernant certaines méthodes. Le souci de limiter le champ d'action d'une plateforme d'échanges conduit à désapprouver certaines méthodes. Par exemple, on ne peut admettre la mise en place d'une plateforme et d'un réseau à compétence résiduelle intervenant dans les cas où aucune autre plateforme n'est compétente.

Ainsi, l'*« Intégrateur de Services fédéral »* dont le rôle est assumé par le SPF Fedict ne peut être encouragé[766]. Il s'agit d'une plateforme d'échanges,

---

[761] Voy. *infra* n°s 599.- et s.

[762] P. TRUDEL, « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *op. cit.,* p. 265.

[763] CPVP, avis n° 41/2008 du 17 décembre 2008 concernant l'avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de Services fédéral, p. 5, n° 14 ; CPVP, recommandation n° 03/2009, *op. cit.,* p. 10, n° 34.

[764] CPVP, recommandation n° 03/2009, *op. cit.,* p. 10, n° 34.

[765] Ce point sera davantage développé dans le titre 2 sur la transparence.

[766] Cet intégrateur de services est organisé par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral.

assumant également le rôle d'intégrateur de services, dont le champ d'action n'est pas assez limité à nos yeux. En effet, cet intégrateur dispose d'une compétence résiduelle puisqu'il est compétent pour tous les services publics fédéraux qui ne sont pas déjà servis par la Banque-Carrefour de la Sécurité sociale ou la plate-forme *eHealth*[767].

> Etonnamment, la CPVP s'est prononcée favorablement sur cet avant-projet de loi, qui a, depuis lors, été adopté. La CPVP a estimé notamment que « l'avant-projet délimite clairement le terrain d'action de l'Intégrateur de Services fédéral par rapport à celui des autres intégrateurs de services actifs au niveau fédéral et régional comme la Banque-Carrefour de la sécurité sociale, la plate-forme eHealth, Easi-Wal, Corve »[768]. Un champ d'action clairement délimité n'en est pas pour autant suffisamment limité, ce que la CPVP manque malheureusement d'examiner.

Dans le même sens, l'étendue du *réseau de la Banque-Carrefour de la sécurité sociale* est si large qu'on en vient à se demander quelles sont les institutions qui n'en font pas partie. On ne peut en effet considérer que le champ d'action de la Banque-Carrefour de la sécurité sociale est suffisamment limité pour que cet outil soit proportionné, compte tenu du fait que, d'une part, le Roi peut étendre la notion de sécurité sociale[769] et que, d'autre part, Il peut également étendre « à d'autres personnes que les institutions de sécurité sociale, tout ou partie des droits et obligations résultant de la présente loi et de ses mesures d'exécutions »[770]. Entre autres nombreux exemples, on constate ainsi, avec un étonnement certain, que les institutions des Communautés et des Régions qui œuvrent pour la protection de la jeunesse, en ce compris la protection judiciaire, font partie du réseau de la sécurité sociale et sont assimilées à des institutions de sécurité sociale. Les données qu'elles traitent dans ce cadre sont considérées comme des données sociales et l'exécution de leurs missions doit être considérée comme une application de la sécurité sociale[771]. On peine à trouver un lien avec le réseau de la sécurité sociale qui visait initialement

[767] Art. 2, 10°, de la loi du 15 août 2012 ; CPVP, avis n° 41/2008, *op. cit.,* p. 5, n° 13.

[768] *Idem.*

[769] Art. 2, dernier al., de la loi du 15 janvier 1990.

[770] Art. 18, al. 1er, de la loi du 15 janvier 1990.

[771] Art. 2 et 3 de l'arrêté royal du 16 janvier 2002 relatif à l'extension du réseau de la sécurité sociale à certains services publics et institutions publiques des Communautés et des Régions, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale. Signalons que la Commission de la protection de la vie privée s'était prononcée défavorablement à propos de cet arrêté royal estimant notamment que l'extension du réseau était disproportionnée. Malheureusement, son avis n'a pas été suivi. Sur cet avis voy. CPVP, avis n° 13/99 du 12 avril 1999 concernant un projet d'arrêté royal relatif à l'extension du réseau de la sécurité sociale à

à regrouper les branches de la sécurité sociale relevant pour la plupart du « Ministère de la Prévoyance sociale et au sein desquelles la sécurité sociale des travailleurs salariés constitue l'élément prépondérant »[772]. Plus d'un citoyen sera également étonné de constater, à la lecture des données enregistrées à son sujet dans le répertoire des références de la Banque-Carrefour de la sécurité sociale, qu'est reprise, par exemple, l'indication suivant laquelle il détient une télévision.

Le même argument peut être invoqué à l'égard de la loi relative à la *plateforme Ehealth*. L'étendue du réseau au sein duquel œuvre la plateforme est déterminée principalement par les termes « soins de santé ». Trop d'institutions sont susceptibles d'être visées par ces termes pour que l'on puisse considérer que l'étendue du réseau est raisonnable. On regrette d'ailleurs que cet argument n'ait pas été invoqué lors du recours intenté contre cette loi auprès de la Cour constitutionnelle.

2. La détermination des fournisseurs et des destinataires des données

186.- Sources authentiques et administrations destinatrices. Concrètement, le législateur doit déterminer l'étendue du réseau sectoriel en identifiant les fournisseurs et les destinataires des données[773].

Pour déterminer les fournisseurs de données, la loi doit énumérer les sources authentiques de données qui font partie du réseau. Les données circulant dans le réseau sont en effet issues des sources authentiques qui, de ce fait, en sont les fournisseurs.

Par ailleurs, la loi doit énumérer les destinataires des données. Si la loi énumère les administrations qui composent le réseau, elle créerait une subdivision fort rigide dans la structure de l'administration. Cela pourrait être considéré comme une atteinte à la compétence du Roi d'organiser l'administration générale. Il est donc préférable que le législateur dresse la liste des missions légales correspondant à la finalité-mère du réseau et prévoie que seules les administrations poursuivant ces missions légales peuvent être destinataires des données, à charge pour le Roi, de dresser la liste de ces administrations.

---

certains services publics et institutions publiques des Communautés et des Régions, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale.

[772] Projet de loi relatif à la loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, Exposé des motifs, *Doc. Parl.*, Ch. Repr., sess. 1988-1989, n° 899/1.

[773] En ce sens, CPVP, avis 14/2010, *op. cit.*, p. 4, §§ 9 et 10.

B. Les sources authentiques de données

187.- Considérations générales. Tout comme la plateforme d'échange de données, une source authentique de données est un outil de traitement qui constitue, de ce fait, une ingérence dans la protection de la vie privée des citoyens. Les éléments essentiels de cet outil doivent être déterminés par le législateur.

188.- L'intérêt d'une source authentique de données. D'innombrables données sont échangées entre les administrations. Pourtant, toutes les informations échangées ne sont pas nécessairement issues d'une source authentique de données. C'est le cas, entre autres exemples, des données relatives au revenu des citoyens, détenues par le SPF Finances. Il a été souligné plus haut[774] que cette information est souvent nécessaire à l'exécution des tâches d'administrations diverses. Pourtant, bien qu'elles soient souvent réutilisées, ces informations ne sont pas enregistrées dans une source authentique. Cette situation de fait pose question au regard des garanties de qualité que doivent respecter les données souvent réutilisées et de la responsabilité qui doit s'en suivre en cas de manquement à ce devoir. Prévoir que les données échangées doivent toutes être issues d'une source authentique de données prend dès lors tout son sens.

§1. La finalité de la source authentique de données

189.- Finalité interne et finalité externe. Rappelons-le, une particularité majeure de la source authentique est de contenir des données qui sont réutilisées par un maximum d'administrations. Cette base de données d'un type particulier poursuit donc une double finalité. L'une est interne, l'autre est externe.

Comme toutes les bases de données de l'administration, la source authentique est avant tout l'instrument de travail de l'administration qui en est responsable. Dans cette optique, elle poursuit une finalité que l'on qualifie d' « interne », puisqu'il s'agit de la finalité poursuivie par cette seule administration. Elle doit être définie de manière déterminée et explicite, en respectant les critères énoncés dans les lignes qui précèdent.

La source authentique poursuit également une finalité « externe », se déployant en dehors des murs de l'administration qui en est responsable. Elle est liée à l'optique de réutilisation des données dans laquelle la source authentique est conçue dès son origine. La finalité « externe » peut être

[774] Voy. *infra,* n° 151.-

formulée plus souplement que la finalité interne. En effet, il ne conviendrait pas de détailler dans la loi chaque finalité poursuivie par chaque administration impliquée dans les échanges que ces outils organisent. Outre le fait qu'il s'agirait d'une démarche rigide, peu adaptée aux évolutions éventuelles des outils en question, cela aurait pour effet d'alourdir fortement les normes concernées, les rendant peu compréhensibles.

Dès lors, on peut admettre, à la suite de la CPVP, que cette finalité se réduise à l'indication du ou des « domaine(s) législatif(s) » dans la limite desquels la source authentique peut être utilisée[775]. En d'autres termes, il s'agit d'indiquer le ou les domaines du droit, rencontrés par une ou plusieurs législations, dont la mise en œuvre justifie l'accès aux données de la source authentique.

> Par exemple, la source authentique des permis de conduire qui sera prochainement créée poursuit, d'une part, une finalité interne. Il s'agit pour le SPF Mobilité des mêmes finalités que celles poursuivies jadis par le fichier central des permis de conduire[776], à savoir, notamment, le contrôle des conditions pour l'obtention du permis de conduire. Elle poursuit, d'autre part, une finalité externe, étant la source authentique de toutes les données relatives au permis de conduire. Il y a donc lieu d'indiquer dans la loi les domaines législatifs concernés. En l'occurrence, il s'agit de la législation en matière de mobilité et de transports (réglementation liée aux permis de conduire, réglementation des transports), de justice, d'environnement, et d'études scientifiques[777].

§2. La proportionnalité de la source authentique de données

190.- La limitation des données et la désignation du responsable de la source authentique. Le contenu de la source authentique doit être limité à certaines données. Par ailleurs, la désignation, par le législateur, d'un responsable de la source authentique apparaît comme une exigence formelle de proportionnalité[778].

---

[775] CPVP, avis n° 07/2002, *op. cit.,* p. 6, n° 11 ; avis n° 42/2006, *op. cit.,* p. 5, n° 16 ; avis n° 14/2010 du 31 mars 2010 relatif à un avant-projet de loi portant création de la Banque-Carrefour des permis de conduire, p. 3, n° 6.

[776] Celui-ci est organisé par l'arrêté royal du 23 mars 1998 relatif au permis de conduire, *M.B,* 30 avril 1998, p. 13483.

[777] CPVP, avis n° 14/2010, *op. cit.,* p. 3, n° 6.

[778] Selon Sébastien Van Droogenbroeck, aux exigences substantielles de la proportionnalité s'ajoutent certaines exigences formelles, qui consistent en des garanties procédurales qui entourent la mesure créant l'ingérence dans la protection de la vie privée. À titre d'exemple, il cite notamment l'intervention d'un « observateur indépendant » lors d'une perquisition menée dans un cabinet d'avocat. Pour cette raison, il nous est apparu opportun de

1. La limitation des données de la source authentique

191.- Les données nécessaires à plusieurs administrations. Une attention particulière doit être portée aux données enregistrées dans la source authentique, qui doivent se limiter aux seules les informations utiles à plusieurs administrations. Une base de données qui ne serait utile qu'à une seule administration n'aurait pas de raison d'être une source authentique de données.

> C'est d'ailleurs ce qu'affirme le décret flamand du 18 juillet 2008 relatif à l'échange électronique de données administratives qui, en son article 2, 2°, caractérise la source authentique de données comme un fichier de données qui est « utile ou nécessaire dans le cadre de l'échange électronique de données administratives ».

Pour identifier ces données, il pourrait être judicieux d'analyser les fichiers et les données existant au sein des administrations et d'identifier les plus consultés. Ceux-là pourraient être transformés en source authentique pour les administrations qui y recourent fréquemment. C'est d'ailleurs la démarche adoptée lors de l'élaboration du Registre national.

> Pour sélectionner les informations les plus pertinentes à enregistrer dans le futur Registre national, 59 fichiers nationaux ont été analysés. Cette étude a permis de faire apparaître les données de la population les plus consultées par les administrations du pays[779].
>
> À partir de ces indications, le législateur a retenu, en 1983, « les informations de base les plus communes »[780] à savoir, les *nom* et *prénoms*, le *lieu* et la *date de naissance*, le *sexe*, la *nationalité* et l'*adresse*. À cela, il a ajouté le *lieu* et *la date du décès*, la *profession*, l'*État civil* et la *composition du ménage*, avançant que « ces informations doivent [...] être communiquées sans retard à certains

mentionner la désignation d'un responsable de la source authentique dans le point consacré à la proportionnalité. [S. Van Droogenbroeck, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme. Prendre l'idée simple au sérieux*, Bruxelles, Bruylant, Publ. FUSL, 2001, p. 313-316].

[779] Parmi les fréquences relevées, 98 % concernaient les nom et prénoms, 93 % concernaient l'adresse, 78 % concernaient la date de naissance, 59 % concernaient le sexe, 54 % concernaient la nationalité, 44 % concernaient le lieu de naissance, 41 % concernaient l'État-civil, 36 % concernaient le groupe linguistique, 32 % concernaient le nom de l'époux(se), 25 % concernaient la profession, 22 % concernaient le numéro de pension et 12 % concernaient le décès [*Doc. Parl.,* Sénat, sess. Ord. 1981-1982, n° 296/1, p. 3].

[780] *Doc. Parl.,* Sénat, sess. Ord. 1981-1982, n° 296/1, p. 3.

> services pour éviter des paiement indus et des frais de recouvrement »[781]. Ces informations sont consacrées à l'article 3 de la loi[782].

Une fois les données délimitées, celles-ci pourront, au besoin, être précisées par le Roi. Dans le cadre de son pouvoir d'exécution des lois, Il est compétent pour définir des « types d'informations » relatives à chaque donnée légale.

> Rappelons que c'est une méthode utilisée pour préciser les données enregistrées au Registre national. Par exemple, la mention « plurinationalité », ajoutée au Registre national par un arrêté royal, précise la donnée « nationalité », qui est une des données légales du Registre national[783].

192.- Une source unique. Il faut encore s'assurer que ces données ne sont pas déjà enregistrées dans une autre source authentique. La source authentique est, en effet, créée pour offrir des données uniques et mettre fin aux copies qui circuleraient. Elle ne peut donc elle-même constituer la copie d'une autre source authentique au risque de générer des erreurs.

La CPVP admet tout de même une exception à ce principe lorsque la finalité poursuivie par les sources authentiques contenant la même donnée est à ce point différente que les informations qui « occupent une position centrale » dans la source authentique ne sont pas les mêmes. Il est dès lors permis de constituer une nouvelle source authentique de données à partir de données figurant déjà dans d'autres sources authentiques. Ce faisant, la nouvelle base de données constitue un « intégrateur de données »[784].

> Par exemple, la donnée « adresse » des citoyens est enregistrée au Registre national. Elle l'est aussi, pour les entreprises, dans le registre de la Banque-Carrefour des Entreprises. La CPVP a admis qu'elle soit également reprise dans la nouvelle source authentique de données qu'est le Fichier Central

---

[781] *Ibid.*, p. 4.

[782] Signalons qu'avant d'être organisé légalement, le Registre national contenait 8 données supplémentaires, ce qui en a amené certains à dire que la consécration légale du Registre national constituait « une régression » et en a poussé d'autres à demander si l'on pouvait « éluder l'argument visant à la protection de la vie privée » car il était « absurde de limiter le nombre de données précisément au moment où la participation au Registre national deviendrait obligatoire » [*Doc. parl.,* Sénat, sess. Ord., 1982-1983, n° 296/2, pp. 5 et 6].

[783] Au sujet des « types d'information », voy. *supra,* n° 111.-

[784] CPVP, recommandation 03/2009, *op. cit.,* p. 2. Voy. *infra*. La Commission y définit l'intégration de données à caractère personnel comme « l'agrégation de données à caractère personnel provenant de plusieurs sources authentiques et leur enregistrement dans une banque de données intégrées distincte, en vue de leurs communication à des tiers ».

d'Adresses de Références (FCAR)[785]. En effet, « dans le FCAR, l'adresse occupe une position centrale, alors que [...] dans le Registre national, c'est l'enregistrement de la personne physique qui est central et dans la Banque-Carrefour des Entreprises, c'est l'enregistrement d'entreprises qui sert de finalité de base [...]. Le FCAR reprend aussi la composante spatiale des adresses (coordonnées xy), ce qui représente une toute nouvelle dimension par rapport aux autre sources authentiques de données dans lesquelles sont également enregistrées les adresses »[786].

2. La désignation du responsable de la source authentique

193.- Garantir la qualité des données. La désignation du responsable de la source authentique importe pour garantir la proportionnalité de l'outil. En effet, c'est à lui qu'il revient d'assurer la qualité des données de la source authentique. Si les données utilisées ne sont pas de qualité, c'est la proportionnalité de l'outil qui est atteinte, puisqu'en fournissant des données qui, fausses, ne sont ni pertinentes, ni adéquates, la source authentique créerait une atteinte à la protection de la vie privée des personnes concernées.

En confrontant les lois sectorielles instaurant des sources authentiques de données, on constate qu'il existe deux méthodes différentes pour désigner le responsable de cet outil : la « répartition fonctionnelle » effectuée par le Roi, et la désignation du responsable de traitement par le législateur.

194.- « Répartition fonctionnelle ». La méthode actuellement la plus utilisée est celle de la « répartition fonctionnelle ». Elle consiste, pour le législateur, à confier au Roi, ou au gouvernement de l'entité fédérée, le soin de désigner l'administration auprès de laquelle est hébergée la source authentique de données. Cette administration doit être considérée comme le responsable de la source authentique de données.

Par exemple, l'article 14 de la loi sur la Banque-Carrefour des véhicules prévoit que « le Roi désigne, après avis du comité sectoriel, les services qui sont chargés [...] selon la répartition fonctionnelle qu'Il fixe, de la collecte primaire et de la tenue à jour des données [...] ».

Si cette méthode respecte la compétence exclusive du Roi d'organiser les services de l'administration générale, elle porte cependant atteinte à

[785] Décret flamand du 8 mai 2009 relatif au Fichier Central d'Adresses de référence (Centraal Referentieadressenbestand), *M.B.*, 1er juillet 2009.

[786] CPVP, avis n° 36/2008 du 26 novembre 2008 concernant le projet de décret relatif au Centraal Referentieadressenbestand (fichier central d'adresses de référence), p. 5, n° 13.

la prévisibilité du traitement et paraît donc peu conforme à l'exigence de légalité imposée à l'article 22 de la Constitution. En effet, tout citoyen doit pouvoir connaître sans difficulté l'administration qui détient la source authentique et qui est chargée d'en assurer la qualité. En cas d'erreur affectant la donnée, il doit pouvoir invoquer la responsabilité d'une administration déterminée. En outre, il doit également pouvoir connaître aisément l'administration responsable de la source authentique pour pouvoir exercer ses droits d'accès et de rectification auprès de celle-ci[787].Ces impératifs semblent, pour l'heure, difficilement atteints par l'intermédiaire d'arrêtés royaux ou de gouvernement.

> L'article 9 de la loi sur la Banque-Carrefour de la sécurité sociale affirme que « la Banque-Carrefour peut, après avoir pris l'avis de son Comité général de coordination, répartir les tâches d'enregistrement des données sociales de manière fonctionnelle entre les institutions de sécurité sociale. Ces institutions sont dans ce cas tenues d'enregistrer dans leurs banques de données sociales et de tenir à jour les données dont la conservation leur est confiée ».
>
> L'interprétation et la mise en œuvre de ce texte se heurtent à des embûches fameuses. Par exemple, si l'on cherche à savoir pourquoi l'extrait de notre répertoire des références communiqué par la BCSS mentionne le fait que nous avons une télévision et/ou si l'on souhaite rectifier cette information, on contactera la Banque-Carrefour pour savoir à qui s'adresser. Celle-ci répondra qu'étant un habitant de la Région wallonne, il faut contacter le Commissariat wallon Easi-Wal. Qui répondra qu'il n'est pas le responsable de la source authentique des données relatives à la radio-télé redevance et qu'il faut contacter la Cellule fiscale de la Région wallonne. Celle-ci répondra qu'elle n'est pas le responsable de ladite source authentique mais qu'il s'agit de la Cellule administrative transitoire pour la gestion de la fiscalité wallonne. Qui n'existe plus. Finalement, on apprendra qu'il faut contacter le Service public de Wallonie, et plus particulièrement la Direction générale opérationnelle de la Fiscalité, Département fiscalité spécifique, Direction de l'Établissement de la fiscalité spécifique. Qui mettra un temps certain à vérifier qu'elle héberge bien cette source authentique et puis, qui s'interrogera sur la qualité des informations, ce qu'elle n'aura pas dû faire régulièrement car ce type de demande est rare, ce que l'on comprend vu la dose de motivation dont il faut disposer pour parvenir à connaître la simple identification du responsable de la source authentique...

195.- Désignation par le législateur. Face aux difficultés générées par la méthode de la répartition fonctionnelle, il paraît préférable d'opter pour la deuxième méthode, qui consiste à laisser au législateur le soin

[787] Voy. *infra,* Titre II.

de désigner le responsable de la source authentique. Celle-ci est plus conforme à l'article 22 de la Constitution.

En outre, cette désignation devrait être effectuée dans la loi instituant à la source authentique de données, et non dans la loi organisant la plateforme d'échanges d'informations entre les différentes sources authentiques d'un même réseau. L'identification du responsable de traitement de la source authentique serait ainsi plus claire.

> C'est la méthode appliquée par le décret flamand du 8 mai 2009 relatif au Fichier central d'Adresses de Référence (CRAB), qui est, rappelons-le, une source authentique d'adresses. Ce décret mentionne, en son article 5, que « l'agence est chargée de la coordination, de la création et de la mise à jour, la gestion et la communication du CRAB, visé dans le présent décret ». L'article 2, 23°, de ce décret définit l'agence comme « la 'Agentschap voor Geographische Informatie Vlaanderen', créée par le décret du 7 mai 2004 portant création de l'agence autonomisée externe de droit public « Agentschap voor Geografische Informatie Vlaanderen' ».

C. Les numéros d'identification

196.- Un identifiant nécessaire. L'attribution d'un ou de plusieurs numéros d'identification à chaque citoyen est directement liée à la mise en place d'un État en réseaux fondé sur des plateformes d'échanges et des sources authentiques de données. En effet, pour que les données soient échangées entre les administrations sans erreur liée à une confusion entre citoyens, il importe que ceux-ci soient identifiés de manière univoque. L'utilisation du nom n'étant pas suffisante, le recours à un numéro d'identification est nécessaire[788].

L'utilisation d'un tel numéro constitue un risque pour la protection de la vie privée. D'une part, cette information rend possible l'interconnexion des fichiers de l'administration. À partir de ce numéro, on peut en effet accéder aux données personnelles des citoyens disséminées dans les différentes institutions et ainsi dresser son profil général. Le pouvoir de l'administration sur le citoyen est considérablement renforcé et l'on craint que les administrations accèdent à des données que leurs missions légales ne

[788] Pour une analyse historique de l'introduction du numéro d'identification dans les États, voy. N. Vandezande, D. De Cock, J. Dumortier, « ID-FIX: IDentification and Federal Interadministration eXchange – eindrapport », Belspo, 2010, pp. 15-28.

justifient pas[789]. D'autre part, ce numéro peut être signifiant et révéler de lui-même des informations personnelles.

> Par exemple, en Belgique, on peut connaître la date de naissance et le sexe du citoyen à partir de son numéro d'identification au Registre national[790].

197.- Numéro universel ou sectoriel ? Si cet outil présente de grands mérites en termes d'efficacité administrative, le souci de protéger la vie privée des citoyens impose au législateur de déterminer la finalité de ce numéro et les conditions de son utilisation, respectueuses de l'exigence de proportionnalité. La finalité et la proportionnalité du numéro d'identification varient selon que ce numéro est unique ou sectoriel.

Rappelons que le numéro d'identification universel, dit aussi « unique », est un identifiant dont l'utilisation est généralisée au sein de l'administration voire étendue au secteur privé. En d'autres termes, à chaque citoyen correspond un seul numéro quelle que soit l'administration concernée.

À la différence du numéro d'identification universel, le numéro d'identification sectoriel est lié, comme son nom l'indique, à un secteur de l'administration. Dans un État en réseaux, le numéro d'identification sectoriel est utilisé au sein d'un réseau sectoriel déterminé à l'exclusion de tout autre.

§1. La finalité du numéro d'identification

198.- Une imprécision inévitable. La finalité du numéro d'identification se déduit de sa nature. S'il s'agit d'un numéro d'identification universel, la finalité de son utilisation se confond avec les missions de toutes les administrations. S'il s'agit d'un numéro d'identification sectoriel, la finalité de son utilisation se réduit aux missions accomplies par les administrations faisant partie du réseau sectoriel concerné.

À nouveau, comme pour les plateformes d'échanges de données et les sources authentiques, la finalité poursuivie par un numéro d'identification ne peut être formulé de manière très précise étant donné que ce numéro est utilisé par plusieurs administrations poursuivant des missions différentes. Enumérer toutes les finalités de toutes les administrations pouvant utiliser ce numéro rendrait la loi rigide et difficile à lire.

---

[789] R. Leenes et B.-J. Koops, « 'Code' and privacy or how technology is slowly eroding privacy' », *in Coding regulation. Essays on the Normative Role of Information technology* (dir. E. Dommering et L. Asscher), La Haye, TMC Asser Press, 2006, p. 179 ; N. Vandezande, D. De Cock, J. Dumortier, *op. cit.*, p. 29.

[790] Voy. *supra*, n° 30.-

199.- L'utilisation du critère fonctionnel. Bien qu'une certaine largesse doive être admise, il s'impose de définir la finalité du numéro d'identification à l'aide d'un critère fonctionnel et non organique[791]. En d'autres termes, il faut relever dans la loi les missions justifiant son utilisation et non seulement la nature de l'administration pouvant l'utiliser.

C'est d'ailleurs un des reproches adressés à la loi sur le Registre national qui énumère les institutions susceptibles d'obtenir du comité sectoriel du Registre national le droit d'utiliser le numéro d'identification du Registre national[792]. La CPVP désapprouve cette méthode, jugeant que « bien que le Registre national ait été créé pour les administrations publiques, ce n'est pas la nature de ces institutions qui justifie qu'elles aient accès à ce registre, mais les missions de service public qu'elles poursuivent et le gain d'efficacité et de sécurité administrative obtenu »[793].

L'utilisation élargie du numéro d'identification du Registre national, autorisée aux fins les plus diverses, témoigne de la faiblesse de cette disposition censée en limiter l'usage. En 1998 déjà, la CPVP dénonçait la difficulté de savoir qui utilisait ce numéro et à quelles fins. À titre d'exemple, elle évoquait les 200 arrêtés royaux qui autorisaient à l'époque l'utilisation de ce numéro[794]. Aujourd'hui, les choses ne sont pas plus claires, quand on constate que chaque année, le comité sectoriel du Registre national rend entre 50 et 70 décisions relatives à l'utilisation de ce numéro. Par ailleurs, les autorisations d'utilisation du numéro du Registre national renferment également bien souvent l'autorisation d'accéder au contenu du Registre national ce qui ne facilite pas la compréhension de ces textes.

Seule une loi claire, portant spécifiquement sur cet identifiant, en en limitant l'usage à l'accomplissement de finalités déterminées à partir d'un critère fonctionnel et explicitement détaillées dans le texte, pourrait encadrer cet outil. Par ailleurs, la clarté dans l'utilisation du numéro d'identification des citoyens serait également confortée par le développement de numéros d'identification sectoriels, comme le détaille l'analyse de la proportionnalité du numéro d'identification.

§2. La proportionnalité du numéro d'identification

200.- Numéro universel ou sectoriel. L'examen de la proportionnalité entre, d'un côté, les avantages offerts par le numéro d'identification en

[791] Voy. *supra,* n° 120.-
[792] Voy. *supra,* n° 31.-
[793] CPVP, avis n° 30/98, *op. cit.,* p. 3, n° 2.
[794] *Idem.*

termes d'efficacité administrative et, de l'autre côté, les risques induits en termes de protection de la vie privée, varie selon que le numéro d'identification est universel ou sectoriel.

1. Le choix entre un numéro universel ou sectoriel

201.- Un équilibre à trouver. Utiliser un identifiant universel facilite les tâches administratives. Il n'y a pas d'hésitation possible puisqu'à chaque citoyen ne correspond qu'un seul numéro. La personne concernée peut même le connaître par cœur et le communiquer aisément aux administrations qui en ont besoin. Par contre, tous les fichiers dans lesquels se trouvent ses données risquent d'être interconnectés. La connaissance de ce numéro pourrait être alors un sésame généralisé[795].

À l'inverse, l'attribution à chaque citoyen de plusieurs numéros d'identification sectoriels risque de ne pas encourager l'efficacité administrative. On craint que ces numéros distincts empêchent l'échange des données. On se demande également comment faire pour que le citoyen se souvienne de ces numéros multiples. Faut-il lui imposer de détenir plusieurs cartes sur lesquelles seraient inscrits ces numéros ? En contrepartie, la vie privée est davantage protégée puisque les risques d'interconnexions sont limités aux seules administrations qui utilisent l'identifiant sectoriel[796]. C'est pourquoi, les numéros sectoriels peuvent être qualifiés de « système préventif » puisqu'ils rendent plus complexes les interconnexions entre fichiers[797].

202.- En Europe en général : la peur d'un numéro universel. La directive 95/46 n'impose pas aux États de choisir un type de numéro plutôt qu'un autre. Elle se contente de prévoir, en son article 8.7, que « les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement ». La directive n'empêche donc pas l'usage d'un identifiant unique. Néanmoins, cette donnée est mentionnée dans la disposition traitant des données sensibles, au même titre que les informations relatives, notamment, à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, aux infractions,

[795] D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen*, Brugge, Vanden Broele, 2005, pp. 57-60 et references citées ; R. Leenes et B.-J. Koops, *op. cit.*, p. 179.

[796] D. De Bot, *op. cit.*, p. 60 ; R. Duaso Cales, *op. cit.*, pp. 157 à 165.

[797] D. De Bot, *Idem.*

aux condamnations pénales, etc. En d'autres termes, sans le dire explicitement, la directive estime que l'utilisation d'un identifiant universel inspire une certaine méfiance.

> Une décision de la Commission européenne des droits de l'homme illustre cette méfiance[798]. Dans cette affaire, un citoyen belge refuse de montrer sa carte d'identité au motif, notamment, que cela porterait atteinte à la protection de sa vie privée. À l'époque, le numéro d'identification au Registre national n'était mentionné sur la carte d'identité que si le titulaire de la carte d'identité en faisait la demande par écrit. La Commission européenne des droits de l'homme estime qu'en l'occurrence, il n'y a pas d'atteinte à la protection de la vie privée puisque l'indication du numéro d'identification est facultative, peu importe que les autres données de la carte doivent y être obligatoirement mentionnées[799]. Cela signifie qu'une attention particulière est accordée à ce numéro d'identification. On peut alors en déduire que le fait que le numéro d'identification du citoyen soit obligatoirement indiqué sur sa carte d'identité, comme c'est le cas aujourd'hui, pose question au regard de la protection de la vie privée.

Plusieurs États européens ont tenu compte de la méfiance qu'inspire l'usage d'un numéro d'identification universel.

> Par exemple, le *Portugal* consacre, dans sa Constitution, l'interdiction « d'attribuer aux citoyens un numéro national unique »[800].
>
> L'utilisation d'un tel numéro est également frappée d'inconstitutionnalité en *Allemagne*. Dans son arrêt du 15 décembre 1983 à propos d'une loi organisant un recensement démographique[801], la Cour constitutionnelle allemande a dégagé un droit à l'autodétermination informationnelle à partir des articles 1 et 2 de la Loi fondamentale allemande qui consacrent les droits à la dignité et à la liberté. Elle affirme expressément dans cet arrêt que l'attribution d'un numéro d'identification universel aux citoyens serait inconstitutionnelle[802].
>
> En *France*, l'évocation d'un identifiant universel fait ressurgir les souvenirs d'un lourd passé. En effet, le NIR[803] a été conçu sous le régime de Vichy. Initialement créé pour classer les fichiers administratifs et effectuer des statistiques démographiques, il a rapidement été utilisé pour distinguer les

[798] Comm. eur. D.H., *Reyntjens c. Belgique,* 9 septembre 1992, n° 16810/90.

[799] *Ibid.*, §2.

[800] Art. 35.5 de la Constitution de la République portugaise du 2 avril 1976.

[801] 65 BVerfGE I, du 15 décembre 1983. Pour une traduction en anglais de cette décision, voy. E. H. Riedel, « Federal Constitutional Court Karlsruhe. Census Act 1983 partially unconstitutional », *Human Rights Law Journal,* 1984, pp. 94 à 116.

[802] 65 BVerfGE I, du 15 décembre 1983, IV, 2, bb.

[803] Numéro d'inscription au répertoire national d'identification des personnes physiques.

« juifs » et les « non-juifs »[804]. On comprend alors l'émotion suscitée en 1970 par le projet SAFARI[805], qui prévoyait l'utilisation généralisée de ce numéro pour permettre l'interconnexion de tous les grands fichiers publics. Cette peur de l'identifiant unique a conduit à l'adoption, en 1978, de la Loi Informatique et Libertés et à la mise en place de l'autorité de contrôle des données française, la CNIL[806]. Celle-ci prône aujourd'hui la doctrine du « cantonnement », selon laquelle « chaque sphère d'activité (fiscalité, éducation nationale, banque, police, …) doit être dotée d'identifiants sectoriels »[807].

203.- En Belgique en particulier : l'utilisation d'un numéro universel. Etonnamment, l'e-gouvernement belge repose actuellement sur l'utilisation d'un identifiant universel. Il s'agit du numéro d'identification du Registre national.

Ainsi, par exemple, ce numéro est utilisé au sein de la Banque-Carrefour de la sécurité sociale[808]. Dans le même sens, l'administration fiscale utilise le numéro fiscal de chaque citoyen, qui est, en fait, le numéro d'identification du Registre national[809]. C'est également ce numéro qui est utilisé par l'intégrateur de service fédéral[810]. Finalement, on aboutit à une utilisation généralisée du numéro d'identification du Registre national qui, pourtant, n'a jamais été discutée comme telle, s'étant développée par étapes progressives[811].

---

[804] CNIL, 20e rapport d'activité, 1999, p. 61, disponible sur le site www.cnil.fr

[805] Système automatisé pour les fichiers administratifs et le répertoire des individus.

[806] CNIL, 20e rapport d'activité, 1999, *op. cit.*, p. 63 ; G. Braibant, « Données personnelles et société de l'information. Rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46 », Paris, La Documentation française, 1998, p. 10.

[807] CNIL, « Conclusions de la Commission nationale de l'Informatique et des Libertés sur l'utilisation du NIR comme identifiant de santé », disponible sur le site www.cnil.fr Voy. égal. D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen, op. cit.,* pp. 66-67.

[808] Art. 7 et 8 de la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale. Pour de plus amples détails, voy. K. Snyders et S. Segaert, « De Onmiddellijke aangifte van tewerkstelling : een sleutelrol voor e-government in de sociale zekerheid », *T.S.R.,* 2003, pp. 93 et 94 ; D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen, op. cit.,* p. 68.

[809] Art. 314, §1, C.I.R. 1992. Pour de plus amples détails, voy. D. De Bot, Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen, *op. cit.*, pp. 68-69.

[810] Art. 5, §1er, de la loi du 15 août 2012 précitée.

[811] X. Huysmans, "General trends with regard to ID Numbers : Belgium", *in* WP 13, *D13.3 : study on ID number policies* (H. Buitelaar éd.), 2007, p. 56 disponible à l'adresse www.fidis-wp13-dell3 3 number_policies_final

D'aucuns soutiennent la généralisation de cet identifiant, et tempèrent ses dangers au motif qu'un comité sectoriel doit en autoriser l'usage au cas par cas[812]. Ils proposent d'améliorer l'utilisation du numéro d'identification du Registre national, notamment en instaurant un cadastre des interconnexions effectuées par les administrations afin d'assurer plus de transparence en cette matière[813].

Cette argumentation ne convainc pas pleinement. En effet, le contrôle effectué par le comité sectoriel du Registre national ne suffit pas à empêcher les abus. Entre autres failles, les critères guidant son analyse sont flous et permettent des interprétations diverses manquant parfois d'objectivité. Des critiques doivent également être émises quant au statut de cet organe de contrôle puisque l'indépendance du comité par rapport à l'administration qu'il est censé contrôler est souvent mise en cause, tout comme la possibilité d'en attaquer la décision[814]. On ne peut dès lors prétendre que le contrôle du comité sectoriel du Registre national suffit à encadrer l'utilisation d'un identifiant universel.

Quant au cadastre d'interconnexions, il reprend la mention des traitements déjà effectués. Cet outil ne permet donc pas d'endiguer, *a priori*, les dangers que représente l'utilisation d'un identifiant universel au sein de l'administration.

204.- Encourager les identifiants sectoriels. Recourir à des identifiants sectoriels paraît préférable. On pourrait prévoir la création d'un numéro d'identification par réseau sectoriel, comme le prône, en France, la « doctrine du cantonnement » défendue par la CNIL[815]. Plus encore, au sein d'un même réseau sectoriel, des « sous-numéros sectoriels » pourraient être créés pour certaines données, telles que les données relatives à la santé, afin de limiter, au sein d'un même réseau, les institutions susceptibles d'avoir accès à certaines données particulièrement protégées[816].

---

[812] N. Vandezande, D. De Cock, J. Dumortier, *op. cit.,* pp. 30, 33 et 34.

[813] *Ibid.,* pp. 68 et s.

[814] Voy. *infra,* n°s 534.- et s.

[815] Voy. *supra,* n° 202.-

[816] X. Huysmans désigne par « context-specific identifiers », le numéro propre à un réseau sectoriel (par exemple le numéro sécurité sociale). Il qualifie de « sector-specific identifiers », le numéro d'identification spécifique au sein d'un même réseau sectoriel (ce serait le cas, par exemple, d'un numéro propre au paiement des allocations familiales). Et de souligner que « the problem [in Belgium] is not so much the non-usage of sector specific identifiers, but the non-usage of context-specific identifiers : the used identifier – the Belgian National Registry number – is not limited to the context of Social Security, either. It is a 'global identifier'". Voy. X. Huysmans, "Legal aspects of global vs. sector-specific identification numbers",

> En ce sens, Yves Poullet encourage l'utilisation d'un numéro d'identification spécifique à certains échanges de données au sein de la plate-forme *E-Health*. Ainsi affirme-t-il « qu'il est clair qu'au sein d'un laboratoire, d'un hôpital, d'une équipe médicale, l'usage d'un identifiant différent tant de celui de la sécurité sociale que de celui de la santé est possible, voire recommandable, chaque fois qu'il apparaît que, pour des raisons de sécurité, il est approprié de veiller à l'étanchéité des traitements en jeu. [...] L'existence d'un numéro d'identification santé n'exclut pas [...] l'existence de numéros plus spécifiques dans le cadre d'applications particulières ou de groupes de professionnels restreints [...] »[817].

À cet égard, la solution autrichienne est intéressante. Chaque citoyen autrichien est enregistré dans le *Zentrales Melderegister (ZMR)* et se voit attribuer un numéro d'identification propre à cette base de données, le numéro ZMR[818]. Ce numéro n'est pas utilisé comme identifiant unique au sein de l'administration. Il sert de numéro source à partir duquel sont dérivés, par un mécanisme de cryptographie, les identifiants sectoriels dont l'utilisation est imposée par la loi autrichienne relative à l'e-gouvernement[819]. Une telle méthode pourrait être utilisée en Belgique à partir du numéro d'identification du Registre national. Il semblerait même qu'elle n'implique pas la mise en place d'une technologie particulièrement couteuse[820].

La CPVP a d'ailleurs proposé l'utilisation d'une méthode semblable pour la création d'un numéro d'identification propre aux traitements de données relatives à la santé. Elle soutient qu' « on pourrait faire usage du numéro du Registre national pour parvenir, au moyen d'un *hashing*, à un nouveau numéro, avec impossibilité pour les instances et les personnes

---

in WP 13, *D13.3 : study on ID number policies* (H. Buitelaar éd.), *op. cit.,* p. 24. Y. Poullet encourage l'utilisation d'un numéro d'identification plus spécifique que le numéro santé, pour certains échanges de données effectués au sein de la plate-forme *E-Health*.

[817] Y. Poullet, « Construire un cadre juridique pour l'e-Health. À propos d'un avant-projet de loi belge en matière de télématique médicale », *in La protection des données médicales. Les défis du XXIème siècle* (dir. J. Herveg), Louvain-la-Neuven Anthémis, 2008, pp. 98-99.

[818] § 16 (1) du *Meldegezets* 1991.

[819] Il s'agit de la *Bundegezets über Regelungen zur Erleichterung des elektronischen Verkehrs mit ôffentlichen Stellen, E-Government-Gesetz*, en vigueur depuis le 1er mars 2004. Cette loi est disponible en version anglaise, *in*titulée Federal Act on Provisions Facilitating Electronique Communications with Public Bodies- Austrian E-government Act sur le site http://www.digitales.oesterreich.gv.at/DocView.axd ?CobId=19380 Voy. spéc. l'art. 6 (2) au sujet du numéro ZMR comme numéro d'identification source.

[820] X. Huysmans, "Legal aspects of global vs. sector-specific identification numbers", *op. cit.,* p. 32.

non habilitées de refaire l'association avec le numéro du Registre national »[821].

2. Le choix entre un numéro signifiant ou non signifiant

205.- Encourager les numéros non-signifiants. Si le législateur s'attèle à réévaluer les numéros d'identification utilisés au sein de l'administration, on ne peut que lui conseiller également de veiller à créer des numéros non-signifiants.

Actuellement, le numéro du Registre national est un numéro signifiant puisqu'il est composé de la date de naissance et d'un chiffre mentionnant le sexe du citoyen (pair pour les femmes, impair pour les hommes). Outre que ce numéro révèle, à sa seule lecture, des informations personnelles, le fait qu'il soit composé d'éléments de l'état civil le rend plus aisé à reconstituer[822]. Il serait donc préférable de recourir à des numéros sans lien avec des caractéristiques personnelles des citoyens. C'est d'ailleurs ce qui a été envisagé lors de la réforme du Registre national en 2003 et encouragé par la CPVP[823]. Malheureusement, cette idée est demeurée un vœu pieu et le temps est venu de la rendre effective.

> Partant du constat que « ce numéro est [...] repris dans de nombreux fichiers et constitue souvent la base du développement du fichier », il a été jugé que « la transformation du numéro national, ainsi que demandé par la Commission de la protection de la vie privée, en un numéro sans référence à des données à caractère personnel exige dès lors une opération qui engendrerait un déséquilibre injustifiable entre les produits (un avantage éventuel pour la protection de la vie privée) et les charges (le travail et les frais) entraînés pour le gestionnaire des fichiers. Il entre toutefois dans les intentions de donner suite pour l'avenir aux observations de la Commission en évoluant prochainement vers un numéro national qui ne contiendrait plus de donnée à caractère personnel »[824].

---

[821] CPVP, avis n° 14/2002 du 8 avril 2002 relatif à un projet d'arrêté royal fixant les normes auxquelles le programme de soins de base en oncologie et le programme de soin d'oncologie doivent répondre pour être agréés, p. 4, n° 7.

[822] CNIL, « Conclusions de la Commission nationale de l'Informatique et des Libertés sur l'utilisation du NIR comme identifiant de santé », précité.

[823] CPVP, avis n° 19/2002, *op. cit.,* p. 8, n° 16, note 5.

[824] Projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personne sphysiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50 2226/001, p. 7.

II. Une loi-cadre

206.- Des traits communs. Le législateur doit organiser la mise en place de chaque réseau sectoriel, composé d'une plateforme d'échanges et de sources authentiques de données, et utilisant un numéro d'identification, comme nous venons de le montrer.

Au-delà des spécificités propres à chaque domaine juridique particulier, on constate que les réseaux sectoriels présentent des traits communs. Pourtant, actuellement, ceux-ci sont réglés par des normes particulières, ce qui génère parfois des *différences* dans la réglementation de principes pourtant semblables.

> Par exemple, le principe de la collecte unique et son corollaire, l'obligation de collecte indirecte des données, sont prévus par la loi sur la Banque-Carrefour de la sécurité sociale[825], la loi sur le Registre national[826], la loi sur la Banque-Carrefour des véhicules[827] et la loi sur la Banque-Carrefour des entreprises[828].

En outre, l'encadrement normatif de l'e-gouvernement souffre de *lacunes*. Entres autres difficultés, on a souligné précédemment que la loi

[825] L'article 11 de la loi du 15 janvier 1990 prévoit que « lorsque les données sociales sont disponibles dans le réseau, les institutions de sécurité sociale sont tenues de les demander exclusivement à la Banque-Carrefour [...] Elles sont également tenues de s'adresser à la Banque-Carrefour lorsqu'elles vérifient l'exactitude des données sociales disponibles dans le réseau ».

[826] L'article 6 de la loi du 8 août 1983 prévoit que « §1er. Les autorités, les organismes et les personnes visés à l'article 5, qui sont autorisés à consulter les données du registre national, ne peuvent plus demander directement lesdites données à une personne. §2. Dès qu'une donnée a été communiquée au Registre national et enregistrée dans ledit Registre, la personne concernée n'est pas tenue de la communiquer directement aux autorités, organismes et personnes visés à l'article 5, qui sont autorisés à consulter les données du Registre national ».

[827] L'article 15 de la loi du 19 mai 2010 prévoit que « lorsque les données relatives aux véhicules sont disponibles dans le réseau, les services sont tenus de les demander exclusivement à la Banque-Carrefour ». L'article 23 de la même loi prévoit que « [...] les services qui sont habilités à consulter les données de la Banque-Carrefour, ne peuvent plus réclamer directement ces données aux personnes physiques ou morales propriétaires d'un véhicule. Dès qu'une donnée est communiquée à et enregistrée dans la Banque-Carrefour, les services habilités à consulter ces données ne peuvent plus, si ces données ne leur sont pas communiquées directement, en imputer la faute à ces personnes ».

[828] L'article 22 de la loi du 16 janvier 2003 prévoit que « des autorités, administrations et services qui sont habilités à consulter les données de la Banque-Carrefour des Entreprises, ne peuvent plus réclamer directement ces données aux entreprises visées à l'article 4 ou aux mandataires de ces derniers. Dès qu'une donnée est communiquée à et enregistrée dans la Banque-Carrefour des Entreprises, les services habilités à consulter ces données ne peuvent plus, si ces données ne leur sont pas communiquées directement, en imputer la faute à l'intéressé ».

du 8 décembre 1992 est particulièrement floue. Il manque également un texte définissant les concepts-clés de cette matière, tels que « plateforme d'échanges d'informations » ou « source authentique de données ».

Enfin, on a constaté les nombreuses *interactions* existantes entre les exigences de droit administratif, d'une part, et celles issues de la protection de la vie privée, d'autre part. Il serait utile de les regrouper dans un seul texte pour les comprendre de manière cumulative et les appliquer aux échanges de données à caractère personnel dans l'administration.

Partant de ces constats, il semble nécessaire d'adopter une loi-cadre organisant la protection des données dans l'e-gouvernement.

207.- Perspective de droit comparé. Plusieurs d'États européens disposent d'une loi qui encadre certains aspects de l'e-gouvernement[829]. Pour la plupart, elles consacrent des mesures techniques visant à assurer la sécurité des données et l'interopérabilité des systèmes. Il y est également question de simplification administrative dans le but d'améliorer les démarches administratives des citoyens. Certaines lois se préoccupent aussi de la collaboration entre les administrations en imposant, par exemple, la collecte indirecte des données.

> Ainsi, la loi autrichienne sur l'e-gouvernement règle notamment l'utilisation du numéro d'identification de chaque citoyen[830].
>
> L'Italie dispose d'un Code d'e-gouvernement, encourageant principalement les administrations à échanger des informations pour simplifier les procédures administratives et à élaborer un portail internet indiquant les services administratifs en ligne, la possibilité de télécharger des documents officiels, etc.[831].
>
> La loi allemande sur la connexion des réseaux informatiques met en place un réseau d'interconnexions au sein duquel les données sont échangées entre les administrations[832].

En général, dans les États européens disposant d'une loi relative à l'e-gouvernement, celle-ci est juxtaposée à la loi relative à la protection

[829] C'est le cas de l'Allemagne, la France, l'Autriche, la Bulgarie, l'Espagne, la Pologne, la Norvège, la Lituanie, l'Italie, l'Islande et la Finlande.

[830] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz-E-GovG du 1er mars 2004, disponible en version anglaise à l'adresse http://digital.austria.gv.at/DocView.axd ?CobId=31191

[831] *Codice dell'amministrazione digitale* du 7 mars 2005, disponible à l'adresse http://www.digitpa.gov.it/amministrazione-digitale/CAD-testo-vigente

[832] Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – (IT-NetzG) du 10 août 2009.

des données à caractère personnel qui transpose la directive 95/46, si bien qu'au moins deux textes doivent être consultés pour connaître les droits et obligations des administrations et des citoyens. Il serait préférable de ne pas suivre cette voie pour réglementer l'e-gouvernement en Belgique. En effet, les analyses menées dans le cadre de cette étude ont montré combien la protection de la vie privée sous-tend l'organisation de l'e-gouvernement. Elle doit dès lors être envisagée dès la mise en place des outils de traitements de données. Ainsi, la loi-cadre relative à l'e-gouvernement devrait consacrer des règles d'échanges de données qui font la synthèse entre les exigences du droit administratif et les impératifs de protection de la vie privée.

208.- Cinq points. La loi-cadre relative à l'e-gouvernement pourrait s'articuler en cinq points.

Premièrement, le modèle suivi est affirmé et les outils de traitement de données sont définis.

Deuxièmement, une signification claire des exigences de finalité et de proportionnalité dans l'administration est établie

Troisièmement, les règles applicables à l'administration demanderesse des données sont déterminées.

Quatrièmement, les règles applicables à l'administration émettrice des données sont posées.

Cinquièmement, les règles de contrôle des échanges au sein d'un réseau sectoriel et entre des réseaux sectoriels sont instaurées.

A. Le modèle et les définitions

209.- Une affirmation claire du modèle d'e-gouvernement. Il importe que le législateur affirme clairement le modèle d'e-gouvernement suivi en Belgique, à savoir, le modèle de l'État en réseaux, décrit précédemment. Certes, la hiérarchie des normes empêche que la loi-cadre relative à l'e-gouvernement s'impose aux autres normes de valeur législative qui seront adoptées ultérieurement pour régler, notamment, les sources authentiques de données et les plateformes d'échanges d'informations. Décrire le modèle d'e-gouvernement dans la loi-cadre ne pourrait dès lors suffire à garantir qu'il soit concrètement suivi. Mais une telle affirmation aurait le mérite d'établir clairement l'orientation prise pour le développement de l'e-gouvernement, dans laquelle devraient s'inscrire les lois postérieures.

210.- Des définitions. La description légale du modèle de l'État en réseaux devrait être accompagnée d'une définition des concepts clés de

cette matière. On pense, par exemple, aux notions de source authentique de données, de plateforme d'échanges d'information, de numéro d'identification, de réseaux sectoriels mais aussi à celles de répertoire de références et, bien sûr, de données à caractère personnel.

> À cet égard, le décret du 18 juillet 2008 relatif à l'échange électronique de données administratives illustre l'intérêt de définir les notions cardinales de l'e-gouvernement. En son chapitre 1er intitulé « Dispositions générales et définitions », il contient notamment la définition de « l'échange électronique de données administratives », « source authentique de données, « utilisateur », « Commission de la protection de la vie privée », « traitement », « commission de contrôle », « entités de l'administration flamande », « données à caractère personnel », etc. Ce sont autant de définitions dont le législateur pourrait s'inspirer lors de l'adoption de la loi-cadre relative à l'e-gouvernement.

De cette manière, il existerait une définition de référence auxquelles les normes adoptées postérieurement pourraient renvoyer.

B. Les exigences de finalité et de proportionnalité applicables aux données et aux traitements

211.- Deux solutions. La question se pose de savoir quelle doit être l'articulation entre la loi-cadre relative à l'e-gouvernement et la loi du 8 décembre 1992. Deux solutions s'offrent au législateur.

Soit il se contente de faire figurer, dans la loi-cadre, une disposition déclarant que la loi du 8 décembre 1992 est applicable aux échanges de données dans et entre les réseaux sectoriels.

Soit il reprend, dans la loi-cadre, les dispositions de la loi du 8 décembre 1992 qui sont pertinentes pour les traitements de données au sein de l'administration et, le cas échéant, les précise.

La deuxième solution nous paraît préférable au regard du souci de garantir l'exigence de légalité et de prévisibilité au sein de l'e-gouvernement et ce d'autant plus que la loi du 8 décembre 1992 est, en tant que telle, trop floue pour prétendre encadrer les traitements de données dans le secteur public.

Il y aurait dès lors lieu de reprendre, dans la loi-cadre, les exigences de finalité et de proportionnalité et de les adapter aux préoccupations du secteur public au regard des enseignements dégagés dans le chapitre 2 de cette étude.

§1. L'exigence de finalité

212.- Finalité déterminée, explicite et légitime. La loi-cadre devrait indiquer que tout traitement de données effectué par une administration doit poursuivre une finalité légitime, déterminée et explicite. En cas de réutilisation de données issues d'une source authentique, la finalité nouvelle doit répondre à l'exigence de compatibilité.

En ce qui concerne l'exigence d'une *finalité légitime*, il serait judicieux de reprendre les valeurs mentionnées par la Convention européenne des droits de l'homme, et non l'article 7 de la directive 95/46 qui, rappelons-le, n'énumère pas des finalités légitimes mais des cas d'admissibilité de traitements.

En ce qui concerne l'exigence d'une *finalité déterminée*, la loi-cadre devrait mentionner que toute finalité poursuivie par une administration doit entrer dans les missions qui lui sont légalement dévolues. En outre, cette finalité doit constituer une fin en soi. Enfin, elle doit être définie à l'aide d'un critère fonctionnel et préciser s'il s'agit d'une finalité de gestion administrative, d'une finalité de contrôle ou d'une finalité d'octroi d'un avantage aux citoyens.

En ce qui concerne l'exigence d'une *finalité explicite*, la loi-cadre devrait imposer aux administrations de mentionner la finalité lors de la demande de données à la plateforme d'échanges d'informations.

Enfin, en ce qui concerne la *finalité de réutilisation des données*, la loi-cadre devrait imposer aux administrations de ne pas opérer de traitement de données qui créeraient, pour le citoyen, le sentiment d'être piégé. La loi pourrait indiquer que tel serait le cas d'une réutilisation de données dans un but de sanction ou de contrôle, alors que la collecte initiale visait à octroyer un avantage aux personnes concernées.

§2. L'exigence de proportionnalité

213.- L'indication de critères. La loi-cadre devrait mentionner explicitement l'exigence de proportionnalité, applicable aux traitements et aux données utilisées.

Tout d'abord, la loi devrait indiquer qu'un traitement électronique de données à caractère personnel ne peut être effectué qu'après s'être assuré qu'il n'existe pas de moyen moins attentatoire à la protection de la vie privée des citoyens.

Ensuite, la loi devrait distinguer la proportionnalité du traitement et la proportionnalité des données.

En ce qui concerne la proportionnalité du traitement, la loi devrait indiquer que, dans l'hypothèse où une collecte indirecte de données peut être réalisée, ce type de collecte doit être favorisé. Dans l'hypothèse inverse, l'administration peut recourir à une collecte directe de données auprès des personnes concernées.

En ce qui concerne la proportionnalité des données, la loi devrait affirmer l'obligation pour les administrations d'utiliser des données exactes et à jour. En outre, celles-ci doivent être limitées à ce qui est nécessaire pour exécuter les missions qui leur sont légalement dévolues. À cet égard, si la mention « oui-non » suffit, son utilisation doit être encouragée. Enfin, la durée de conservation des données doit être limitée à ce qui est nécessaire pour l'exécution des missions légales des administrations.

C. Les règles applicables à l'administration demanderesse des données

214.- L' « administration demanderesse ». L'administration demanderesse des données est celle qui demande les informations dont elle a besoin. On l'appelle aussi l' « administration destinatrice » des données.

Les demandes de données adressées par une administration à une autre sont nombreuses, compte tenu du fait que le modèle d'e-gouvernement est fondé la circulation des données, qui suppose le respect d'une obligation de collecte indirecte[833].

La loi-cadre organisant l'e-gouvernement doit affirmer explicitement l'obligation de collecte indirecte et prévoir que la demande de données soit motivée.

215.- L'affirmation explicite de l'obligation de collecte indirecte. Rappelons-le[834], l'obligation de collecte indirecte des données est un corollaire du principe de la collecte unique des données. Cette obligation consiste à imposer aux administrations d'utiliser les données qui, ayant déjà été collectées, sont disponibles dans le réseau sectoriel et de renoncer à les demander directement à la personne concernée.

La loi-cadre relative à l'e-gouvernement doit imposer explicitement aux administrations d'un réseau sectoriel l'obligation de collecter indirectement les données disponibles dans le réseau, qu'elles sont habilitées à connaître en vertu de leurs missions légales et des finalités poursuivies.

---

833 Voy. *supra*, n°s 157.- et s.

834 Voy. *supra,* n° 10.-

216.- La demande des données à la plateforme d'échanges d'informations. La loi-cadre relative à l'e-gouvernement doit imposer aux administrations d'un réseau sectoriel d'introduire leur demande de données auprès de la plateforme d'échanges d'informations de ce réseau. En effet, comme cela a été expliqué précédemment[835], celle-ci dispose d'un répertoire des références qui lui permet d'aller chercher l'information dans l'administration qui la détient et de l'acheminer vers l'administration demanderesse. Cette dernière ne doit donc pas identifier elle-même la ou les source(s) authentique(s) contenant les informations recherchées. En outre, la plateforme d'échanges d'informations peut limiter les données fournies à la mention « oui-non », ce qui améliore la proportionnalité du contenu du traitement. Enfin, la plateforme d'échanges d'informations peut être chargée de certains services, comme l'anonymisation des données échangées.

D. Les règles applicables à l'administration émettrice des données

217.- L' « administration émettrice ». L'administration émettrice des données est celle qui communique les données demandées. Elle est également l'administration responsable de la source authentique contenant ces informations.

Comme on l'a souligné précédemment, il importe que les données de la source authentique soient fiables, ce qui relève de la responsabilité de l'administration détenant la source authentique.

En outre, l'administration émettrice des données doit disposer d'une base légale pour justifier la communication de données, étant donné qu'une administration ne peut agir que dans les limites des compétences qui lui sont légalement dévolues.

La responsabilité de la qualité des données et la compétence légale de communiquer les données sont abordées à présent.

§1. La responsabilité de la qualité des données

218.- Une présomption de qualité des données. L'administration qui détient une source authentique est responsable de la qualité des données qui s'y trouvent. Elle doit tout mettre en œuvre pour garantir que les données émises sont exactes et à jour afin d'éviter la circulation de données erronées.

---

[835] Voy. *supra,* n°s 146.- et s.

À l'obligation de l'administration responsable de la source authentique de garantir la fiabilité des données qui s'y trouvent doit correspondre une « présomption de qualité des données ». En d'autres termes, si une donnée est issue d'une source authentique, elle est présumée fiable.

Cette présomption doit être réfragable. Elle doit pouvoir être renversée par la personne concernée ou par une administration qui constaterait une erreur. Si la présomption de qualité des données est renversée, cela doit entraîner la responsabilité de l'administration détentrice de la source authentique. Ce serait en effet la preuve qu'elle n'a pas accompli son obligation de garantir la fiabilité des données.

On ne peut donc suivre la CPVP quand elle soutient que les sources authentiques appartenant au réseau *eHealth* ne peuvent bénéficier d'une présomption de qualité au motif que « les données qui bénéficient de ce genre de présomption, comme celles du Registre national, sont des données protégées par des procédures d'enregistrement spéciales (constatation par un officier d'État civil, etc.) »[836]. Ce raisonnement revient à réduire la fiabilité des données à un accessoire dont seraient assorties certaines sources authentiques et pas d'autres. Pourtant, bien au contraire, c'est un élément essentiel de cet outil. Sans garantie de fiabilité, on ne peut encourager la réutilisation des données. La qualité de source authentique doit donc être refusée quand la base de données contient des informations dont l'administration ne peut garantir la fiabilité. Dans un cas comme celui de la plateforme *eHealth*, il revient à la CPVP de demander au législateur d'imposer aux administrations responsables d'une source authentique de garantir la fiabilité des données en mettant en place les mécanismes nécessaires à la réalisation de cet objectif. Si cet impératif n'est pas respecté, il s'impose que la qualité de source authentique soit refusée à la base de données mise en place.

219.- Des garanties procédurales. Corollairement à l'obligation de garantir la fiabilité des données, la CPVP suggère de mettre en place certaines garanties procédurales entourant la qualité des données de la source authentique. Il peut ainsi être judicieux que l'administration responsable de la source authentique enregistre les modifications apportées aux données. Ce faisant, on peut savoir, par exemple, à partir de quand la donnée a

[836] CPVP, avis n° 14/2008 relatif à la demande de la Ministre des Affaires sociales et de la Santé publique et de la Ministre de la Fonction publique et des Entreprises publiques concernant un projet de loi portant institution et organisation de la plate-forme *eHealth*, p. 22, n° 94. Notre critique ne porte pas sur les diagnostics médicaux nécessitant l'appréciation d'un médecin, puisqu'un tel diagnostic ne peut bien évidemment pas être « vrai » ou « faux »

été mise à jour et rectifier les éventuelles communications de données qui n'en auraient pas tenu compte. Il y a lieu également d'imposer aux administrations de conserver l'historique de l'accès aux données et de mettre en place un « contrôle de la qualité à l'égard des utilisateurs », c'est-à-dire, un système qui avertit les utilisateurs qu'une donnée communiquée était fautive et a été depuis corrigée[837]. En cas de manquement à ces obligations, la responsabilité de l'administration pourra être engagée[838].

§2. La compétence légale de communiquer les données

220.- Communication légale de données. La circulation des données au sein d'un réseau sectoriel suppose que l'administration détenant la source authentique de données puisse légalement communiquer les informations demandées.

Dès lors, il y a lieu de prévoir explicitement, dans la loi-cadre relative à l'e-gouvernement, que les administrations responsables d'une source authentique de données sont compétentes pour donner les informations demandées par la plateforme d'échanges du réseau sectoriel auquel elles appartiennent.

E. Le contrôle de l'échange de données au sein d'un réseau et entre réseaux[839]

221.- Considérations générales. Il importe de contrôler les échanges de données, qu'ils aient lieu au sein d'un réseau sectoriel ou entre plusieurs réseaux sectoriels. Un tel contrôle peut être organisé à partir d'ententes de partage, comme l'expliquent les développements qui suivent.

§1. Le contrôle des échanges de données au sein d'un réseau sectoriel

222.- Des ententes de partage. Lorsque l'administration demanderesse de données souhaite obtenir des informations enregistrées dans une source authentique de données, elle pourrait prendre contact avec l'institution responsable de la source authentique, afin de rédiger une entente de partage.

---

[837] CPVP, avis n° 11/2009, *op. cit.*, p. 3, n° 9.

[838] Voy. *infra*, n° 401.- et s. (au sujet de l'*audit trail*).

[839] Le troisième titre de l'ouvrage est consacré aux contrôles des traitements de données à caractère personnel. Néanmoins, nous abordons d'ores et déjà le contrôle des échanges au sein d'un réseau et entre réseaux sectoriels afin d'exposer la structure de ce contrôle dans le cadre d'un État en réseaux.

Le mécanisme de l'entente de partage est une solution pratiquée au Québec, notamment[840]. Il fait l'objet de développements détaillés dans le troisième titre de la recherche.

Signalons d'ores et déjà que, tel que nous l'envisageons dans cette recherche, l'entente de partage prend la forme d'un document dans lequel le détaché à la protection des données[841] de l'administration demanderesse prend contact avec le détaché à la protection des données de l'administration émettrice des informations, pour fixer explicitement les conditions du transfert de données, dans le respect des exigences de la loi.

> Selon un commissaire à l'information et à la protection de la vie privée du Canada, « c'est la façon dont les gouvernements devraient travailler dans le souci de servir l'intérêt public. Le gouvernement fédéral croit qu'il peut tout bonnement obtenir auprès d'autres gouvernements et entités connexes tous les renseignements personnes dont il a besoin pour faire son travail. [...] Les ententes de partage de données permettent de bien comprendre la situation, comportent des règles et des responsabilités et assurent la transparence aux fins de la protection de la vie privée »[842].

Ainsi, l'entente de partage devrait reprendre notamment les données transférées, en veillant à respecter l'exigence de proportionnalité. Il devrait mentionner également la finalité du traitement. Rappelons[843] que la finalité du traitement doit être déterminée, explicite et légitime. Il ne faut pas non plus que le citoyen ait l'impression d'être piégé, ce qui serait le cas si des données collectées pour une finalité avantageuse étaient réutilisés dans un but de contrôle.

L'entente de partage devrait également reprendre la ou des base(s) légale(s) justifiant que les données demandées entrent bien dans les missions de l'administration demanderesse.

À ce stade, un premier contrôle du transfert serait donc effectué par les détachés à la protection des données des deux institutions concernées, puisque ces spécialistes de la protection des données seraient chargés de vérifier que l'échange d'informations envisagé respecte les conditions légales.

---

[840] Art. 67 et s. de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. À ce sujet, voy. P. TRUDEL, « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *op. cit.,* pp. 256 à 259.

[841] Le détaché à la protection des données est une personne indépendante, travaillant au sein d'une institution qui traitre des données, et qui est spécialisé dans les règles de protection des données. À ce sujet, voy. *infra,* n°s 552.- et s.

[842] D.H. FLAHERTY, *Réflexions sur la réforme de la Loi sur la protection des renseignements personnels,* Juin 2008, pp. 19 et 20, disponible à l'adresse http://www.priv.gc.ca/information/pub/pa_ref_df_f.pdf

[843] Voy. *supra,* n°s 113.- et s.

223.- La transmission de l'entente à la plateforme d'échange. Une fois l'entente de partage rédigée, elle devrait être transmise à la plateforme d'échanges d'informations. Celle-ci serait chargée d'acheminer les données demandées à l'administration demanderesse.

Un deuxième contrôle des données pourrait ainsi être réalisé puisque, concrètement, la plateforme veillerait à ne transmettre effectivement que les données entérinées dans l'entente de partage.

224.- La transmission de l'entente à la CPVP. L'entente de partage devrait également être transmise à la CPVP.

Cela permettrait d'assurer un troisième contrôle de l'échange, par la CPVP qui serait en mesure de vérifier la légalité de l'entente de partage et de réagir en cas de violation des règles de protection des données.

En outre, la CPVP devrait publier l'entente sur son site internet et s'en servir pour mettre à jour le cadastre des interconnexions[844]. Grâce à ces mesures de transparence, un quatrième contrôle pourrait être effectué par les citoyens qui auraient connaissance des échanges de données opérés, grâce aux mesures de transparence.

D'ailleurs, le commissaire à l'information et à la protection de la vie privée au Canada dont il a été question dans les lignes qui précèdent explique que la transparence rendue possible grâce à la publication des ententes de partage explique que les bureaucrates n'y soient pas très favorables car ils « n'aiment pas devoir négocier de telles ententes parce qu'elles permettent aux commissaires à la protection de la vie privée, aux défenseurs de la vie privée et aux médias, de se faire une idée de ce qui se produit, ou de ce qui est planifié, et d'aider à fixer les règles de base pour la protection des données ».[845]

Toutefois, nous abondons dans le sens de Rosario Duaso Calès qui, dans sa thèse de doctorat consacrée au principe de finalité[846], soutient que la multiplication des ententes de partage pourrait nuire à la transparence des échanges de données. C'est pourquoi, nous soutenons que ces ententes doivent ensuite être reprises dans le cadastre des interconnexions. Elles doivent également être soutenues par des mesures de transparences nouvelles et plus générales. L'ensemble des ces mesures, ainsi que les expli-

[844] Voy. *infra*, n°s 392.- et s.

[845] D.H. Flaherty, *Réflexions sur la réforme de la Loi sur la protection des renseignements personnels, op. cit.*, pp. 19 et 20.

[846] R. Duaso Cales, *Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau*. Thèse de doctorat présentée à la faculté de droit de l'Université de Montréal et à la faculté de droit de l'Université de Paris II, septembre 2011, pp. 273 et 274.

cations relatives au cadastre des interconnexions, sont reprises dans le deuxième titre de cette recherche[847].

Outre que la transmission des ententes de partage permettrait un contrôle de l'échange de données, elle pourrait aussi améliorer l'efficacité administrative. En effet, si la CPVP se sert de ces ententes pour établir le cadastre des interconnexions, on pourrait dégager, à partir de ce cadastre, des catégories de données échangées, en fonction des demandeurs, des finalités, des types de données et des bases légales fondant les traitements. Un tableau clair de ces informations pourrait être dressé, et faciliterait d'ailleurs la lecture des ententes de partage. De telles catégories pourraient être créées ou mises à jour après une certaine période ou un certain nombre de demandes.

Grâce à ce tableau, les administrations pourraient se contenter de motiver leur entente de partage en se référant à une catégorie particulière d'échanges, sans devoir à nouveau justifier la finalité, la proportionnalité et la base légale de la demande. Cela permettrait également aux administrations qui n'ont pas encore accès aux données de prendre connaissance du fait qu'elles pourraient introduire la demande aisément.

§2. Le contrôle des échanges de données en dehors du réseau sectoriel

225.- La particularité des échanges inter-réseaux. Bien que les réseaux sectoriels devraient être conçus de telle manière qu'ils regroupent les administrations appartenant à une même famille de prestations et poursuivant des tâches répondant à une finalité mère commune, certaines données d'un réseau sectoriel seraient appelées à être utilisées au sein d'un autre réseau sectoriel.

> On pense, par exemple, aux données relatives aux revenus des citoyens. Celles-ci servent à établir l'impôt mais également à calculer le montant des allocations familiales, à exonérer certaines personnes de la taxe télé-redevance, etc. Ces problématiques ne feront pas nécessairement partie d'un même réseau sectoriel. Pourtant, elles nécessitent toutes la connaissance du revenu des personnes concernées.

C'est pourquoi, la loi-cadre relative à l'e-gouvernement devrait également envisager l'hypothèse des transferts de données entre deux réseaux sectoriels distincts, que l'on appelle des « transferts inter-réseaux », par opposition aux « transferts intra-réseaux ».

---

[847] Voy. *infra,* n°s 392.- et s.

Les transferts inter-réseaux risquent d'ébranler davantage les attentes raisonnables des citoyens que les transferts intra-réseaux. En effet, comme nous l'avons souligné précédemment, dans le modèle de l'État en réseaux, les citoyens sont conscients que leurs données circulent au sein de réseaux dont l'étendue est clairement délimitée en fonction des facettes de leur vie administrative. En comprenant le fonctionnement de l'administration fondée sur ces réseaux, leur confiance en l'État est confortée. Par contre, ils ne s'attendent pas nécessairement à ce que des données circulant au sein d'un réseau puissent également être utilisées dans un autre réseau. C'est pourquoi, un contrôle renforcé doit être assuré en ce qui concerne les transferts inter-réseaux.

226.- Des ententes de partages approuvées par la CPVP. Comme dans l'hypothèse d'un transfert intra-réseau, un transfert de données inter-réseau devrait être formalisé dans une entente de partage. Les conditions légales devraient y être mentionnées, en portant une attention particulière à la finalité et à la proportionnalité du traitement. Ce dernier point mériterait une attention particulière puisqu'il s'agit d'un transfert entre deux réseaux sectoriels. Il y aurait donc lieu de se demander si une collecte directe de données, effectuée individuellement auprès de chaque personne concernée, ne serait pas préférable pour ne pas heurter la prévisibilité des citoyens.

Cette entente de partage devrait ensuite être communiquée à la plateforme d'échanges du réseau sectoriel dans lequel se trouvent les données recherchées, qui serait ensuite chargée de les acheminer.

Enfin, et surtout, cette entente de partage devrait être communiquée à la CPVP, mais elle devrait également être soumise à l'autorisation de cette autorité de protection des données et ce, avant le transfert effectif des données. La CPVP devrait être contrainte de rendre son autorisation dans un délai raisonnable. On pense au délai d'un mois. Si l'autorisation n'était pas donnée dans ce délai, la CPVP serait présumée accepter le transfert effectué.

En cas d'autorisation, l'échange de données pourrait être effectué. Dans l'hypothèse inverse, la collecte indirecte de données ne pourrait être réalisée.

Un tel contrôle aurait pour but de protéger les données à caractère personnel tout en ne freinant pas exagérément l'efficacité administrative. Il ne pourrait pas non plus remplacer les recours offerts aux personnes concernées, qui seront étudiés dans le troisième titre de la recherche.

III. Des accords de coopération

227.- Considérations générales. Comme l'a mentionné le premier chapitre, tant le législateur fédéral, que les législateurs communautaires et régionaux sont compétents pour organiser des traitements de données à caractère personnel. En effet, le mot « loi » figurant à l'article 22, alinéa 1er, de la Constitution ne s'entend pas exclusivement de la loi fédérale mais vise également les décrets et les ordonnances.

Concrètement, cela signifie que la mise en place des outils de traitement de données, la définition des réseaux sectoriels et l'adoption des règles applicables aux administrations peuvent être réalisées tant au niveau fédéral qu'au sein des entités fédérées. C'est d'ailleurs ce qui se fait déjà progressivement. Certains aspects de l'e-gouvernement sont soumis à des décrets, d'autres, à des lois fédérales qui génèrent une législation parsemée, manquant de clarté et de cohérence. Cette situation est critiquable, comme l'expliquent les développements qui suivent. Une collaboration entre ces autorités est donc nécessaire. Elle peut être concrétisée par la conclusion d'accords de coopération.

A. La justification des accords de coopération dans l'e-gouvernement

228.- Un modèle commun d'e-gouvernement. Bien que chaque entité, fédérale ou fédérée, soit compétente pour organiser l'e-gouvernement, le modèle d'État en réseaux, décrit dans la suite de cette étude, suppose une coopération entre toutes ces entités.

En effet, au sein de la plupart des réseaux sectoriels, devront circuler des informations. Les réseaux sont définis par rapport à une finalité-mère qui correspond à une facette de la vie administrative des citoyens[848]. La détermination des informations ayant vocation à circuler dans ces réseaux se fait donc par rapport à la fonction qu'elles vont remplir, et non plus par rapport au ministère dont elles émanent. Etant donné que des administrations fédérales, communautaires et régionales participent à la réalisation de missions communes, des données provenant de sources authentiques fédérales, communautaires et/ou régionales sont appelées à se retrouver au sein d'un même réseau.

> Ce sera le cas, par exemple, du réseau Impôts et taxes. Y seront impliquées les régions, chargées de percevoir notamment la taxe téléredevance, l'État

[848] Voy. *infra,* n° 177.-

> fédéral, pour les impôts sur le revenu notamment. Pour fixer le montant de ces taxes et impôts, État fédéral et régions auront besoin d'informations identiques circulant au sein du réseau sectoriel Impôts et taxes.

Certes, on pourrait se reposer sur la situation actuelle. Chaque entité continuerait à créer ses outils et à adopter des règles de manière parcellaire, en fonction de leurs besoins propres. Elle trouverait, le cas échéant, quelque arrangement si des données provenant d'une autre entité s'avéraient nécessaires. Cette attitude serait critiquable, pour plusieurs raisons.

a) La vie privée et l'efficacité administrative. L'amas de règles distinctes et éparses serait dangereuse au regard de la protection de la vie privée. Il nuirait à la qualité des normes encadrant l'e-gouvernement. Celles-ci ne seraient donc pas suffisamment prévisible au regard de l'article 22 de la Constitution.

L'efficacité administrative s'en trouverait également affectée. Comment organiser des transferts d'informations efficaces quand les règles de collecte et de communications de données varient en fonction des divisions territoriales ?

> Entre autres exemples, si la Communauté française imposait une exigence de consentement de la personne concernée lors d'un transfert de données, qui s'ajouterait aux exigences de finalité et de proportionnalité, alors que tel ne serait pas le cas de la Communauté flamande, l'administration fédérale chargée d'émettre la donnée demandée devrait se soucier de demander, ou non, le consentement de la personne concernée selon que l'information est émise vers la Communauté française ou la Communauté flamande ?

b) L'exclusivité des compétences. On pourrait également être tenté de régler l'e-gouvernement au niveau fédéral, et d'imposer ensuite aux entités fédérées la loi-cadre relative à l'e-gouvernement ainsi que les lois fédérales qui organisent les sources authentiques de données, les plateformes d'échanges d'informations et l'utilisation des numéros d'identification. C'est une tentation et une tentative que l'on a soulignées à propos de la soumission des normes décrétales au respect de la loi du 8 décembre 1992[849]. Pourtant, rappelons-le, une telle solution serait contraire aux principes qui sous-tendent l'organisation de notre État fédéral et, en particulier, celui de l'exclusivité des compétences.

c) Le principe de proportionnalité dans l'État fédéral. Qu'il s'agisse pour chaque législateur de régler lui-même la matière, ou qu'il s'agisse pour le législateur fédéral d'imposer ses normes aux législateurs

[849] Voy. *infra,* n°s 81.- et s.

communautaires et régionaux, on peut se demander si le fait, pour une entité, d'organiser partiellement le fonctionnement de l'e-gouvernement sans coopération avec les autres autorités, ne porterait pas atteinte au principe de proportionnalité propre à tout exercice de compétence au sein d'un État fédéral. Cette règle de proportionnalité signifie que, dans un État fédéral, « un législateur, fût-il compétent, doit veiller à ne pas rendre impossible ou exagérément difficile, la mise en œuvre par un autre législateur de sa compétence »[850].

Si le législateur fédéral, par exemple, définit lui-même tous les réseaux sectoriels en lien avec l'une de ses compétences, et décide seul des règles régissant la circulation des informations entre les administrations, dans quelle mesure les entités fédérées pourront-elles encore intervenir dans l'organisation de l'e-gouvernement et décider des règles nécessaires pour protéger la vie privée des citoyens ? À ce propos, il est intéressant de constater que la Cour constitutionnelle a déjà annulé plusieurs lois qui réglaient des aspects de l'infrastructure des communications électroniques, au motif que le législateur avait agi de manière unilatérale et avait, de ce fait, violé ce principe de proportionnalité. Bien que la problématique ne soit pas identique à celle de la protection de la vie privée dans l'e-gouvernement, certaines affirmations de la Cour pourraient être transposées à la confection de l'État en réseaux.

> Dans trois arrêts, la Cour considère qu'en agissant de manière unilatérale, le législateur viole le principe de proportionnalité, étant donné que « les compétences de l'État fédéral et des communautés en matière d'infrastructure des communications électroniques sont devenues à ce point imbriquées, par suite de l'évolution technologique, qu'elles ne peuvent plus être exercées qu'en coopération »[851]. Si ces compétences sont imbriquées, explique-t-elle, c'est parce que « les développements technologiques récents ont pour effet que [...] les télécommunications ne peuvent plus être délimitées à l'aide de critères techniques tels que l'infrastructure sous-jacente, les réseaux ou les terminaux utilisés, mais bien sur la base de critères de contenu et de critères fonctionnels »[852], tout comme, en l'occurrence, l'administration d'hier, structurée en silos cloisonnés correspondant à chaque ministère, ne peut être assimilée à l'administration en réseaux de demain.

---

[850] F. Delpérée, *Le droit constitutionnel de la Belgique*, *op. cit.*, p. 592, n° 673.

[851] C.C., arrêt n° 132/2004, du 14 juillet 2004, B.6.2. La Cour rappelle ce passage dans deux arrêts rendus postérieurement au sujet de l'infrastructure en matière de communications électroniques : arrêt 128/2005, du 13 juillet 2005, B.6.2., et arrêt 163/2006, du 8 novembre 2006, B.3.1. Voy. à ce sujet, Y. Lejeune, *Droit constitutionnel belge,* Bruxelles, Larcier, 2010, p. 571, n° 679.

[852] C. C., arrêt n° 132/204, *op. cit.,* B.4.3.

> La Cour précise encore, dans un arrêt rendu ultérieurement à propos de la même problématique, qu'il importe « de faire en sorte que ces autorités harmonisent leurs normes respectives et [d'] éviter que cette infrastructure soit soumise à des dispositions contradictoires »[853].

Dans la lignée de la Cour constitutionnelle, Hugues Dumont affirme que « les répartitions de compétences en dentelle dont nous avons le secret sont aussi un incitant aux accords de coopération : dans plusieurs secteurs, ces accords sont le seul moyen de mener des politiques cohérentes conciliables avec le principe de l'exclusivité des compétences »[854].

Récemment, la Cour constitutionnelle a été saisie d'un recours en matière d'e-gouvernement, qui lui offrait l'occasion d'affirmer l'importance de la collaboration entre les collectivités politiques dans ce domaine. Malheureusement, elle n'a pas appliqué le même raisonnement que dans les arrêts que l'on vient d'évoquer. L'arrêt rendu est décevant car il esquive le problème de l'exclusivité des compétences et du principe de proportionnalité[855].

Au vu de l'importance d'une coopération entre les autorités au sein du modèle de l'État en réseaux et du souci d'éviter des dispositions contradictoires, on peut raisonnablement soutenir que la Cour se prononcerait dans les mêmes termes si un législateur prétendait régler, unilatéralement, le fonctionnement de l'e-gouvernement. La collectivité fédérale et les collectivités fédérées doivent dès lors collaborer pour organiser l'e-gouvernement, ce qui peut être réalisé grâce aux accords de coopération.

B. Les caractéristiques des accords de coopération dans l'e-gouvernement

229.- La notion d'accord de coopération. La collaboration entre l'entité fédérale et les entités fédérées pour organiser l'e-gouvernement peut se concrétiser par l'adoption d'accords de coopération.

Un accord de coopération est une entente, pouvant prendre des formes diverses, entre des collectivités politiques autonomes, par laquelle ces dernières organisent conjointement l'exercice de matières qui relèvent de leurs compétences exclusives[856]. La conclusion de tels accords est organisée

---

[853] C. C., arrêt n° 128/2005, du 13 juillet 2005, B.6.3.

[854] H. Dumont, « L'État belge résistera-t-il à sa contractualisation ? Considérations critiques sur la mode belge des accords de coopération », *Rev. Dr. ULB,* 2006, p. 319.

[855] À ce sujet, voy. *infra,* n° 440.-

[856] T. de Wilde d'Estmael, « Les accords de coopération entre l'État, les Communautés et les régions », *R.R.D.,* 1989, pp. 431 à 441 ; J. Poirier, « Le droit public survivra-t-il à sa contractualisation ? Le cas des accords de coopération dans le système fédéral belge »,

par l'article 92 *bis,* §1, de la loi spéciale du 8 août 1980 de réformes institutionnelles, en vertu duquel « l'État, les Communautés et les Régions peuvent conclure des accords de coopération qui portent notamment sur la création et la gestion conjointes de services et institutions communs, sur l'exercice conjoint de compétences propres, ou sur le développement d'initiatives en commun ».

Les accords de coopération peuvent porter sur toute matière. Il est donc utile d'y recourir pour organiser l'e-gouvernement dans notre État fédéral. C'est l'objet du premier point de l'exposé qui suit.

Le deuxième point s'attache à identifier les auteurs des accords de coopération. Si ces ententes peuvent, certes, être conclues par les gouvernements, l'intervention des législateurs est requise en matière d'e-gouvernement.

Enfin, il convient de s'interroger sur la valeur de ces accords afin de savoir s'ils peuvent être modifiés unilatéralement. Le troisième point est consacré à ces aspects.

§1. L'objet des accords de coopération

230.- Toute matière. Les accords de coopération peuvent porter sur toute matière appartenant aux compétences de la collectivité fédérale, des Communautés et des Régions, du moment que les partenaires respectent « les normes supérieures et notamment les règles constitutionnelles et légales de répartition de compétences », car ces accords ne pourraient aboutir à « un échange, un abandon ou une restitution de compétences telles qu'elles sont déterminées par la Constitution et en vertu de celle-ci »[857].

Ce type d'accord n'est pas inconnu de l'e-gouvernement. En effet, trois accords de coopération ont déjà été conclus dans ce domaine. Ils ont une vocation générale, visant le développement de l'e-gouvernement dans son ensemble. Par ailleurs, d'autres accords sont rendus nécessaires par

Rev. Dr. ULB, 2006, pp. 261 à 314 ; H. Dumont, « L'État belge résistera-t-il à sa contractualisation ? Considérations critiques sur la mode belge des accords de coopération », *Rev. Dr. ULB,* 2006, pp. 315 à 344.

[857] SLCE, avis du 13 juillet 1988 sur un avant-projet de loi « modifiant la loi du 8 août 1980 de réformes institutionnelles », *Doc. Parl.,* Ch. Repr., sess.extr. 1988, n° 5146/1, p. 52. Voy. également F. Leurquin-De Visscher, « Les règles de droit » in *La Belgique fédérale* (dir. F. Delpérée), Bruxelles, Bruylant, 1994, p. 220. Voy. également, F. Delpérée, *Le droit constitutionnel de la Belgique, op. cit.,* pp. 624-625, n°s 721 à 723 ; D. Batselé, T. Mortier et M. Scarcez, *Initiation au droit constitutionnel,* Bruxelles, Bruylant, 2009, p. 465, n° 645 ; M. Uyttendaele, *Trente leçons de droit constitutionnel, op. cit.,* p. 847, n° 11.

certaines lois sectorielles. L'accord de coopération conclu en mai 2013 entre la Région wallonne et la Communauté française s'inscrit en ce sens.

1. Les accords de coopération à vocation générale

231.- Les accords de coopération du 23 mars 2001, du 28 septembre 2006 et du 26 août 2013. Trois accords de coopération ont été conclus et ont une vocation générale. Il s'agit de l'accord du 23 mars 2001 concernant la construction et l'exploitation d'une e-plate-forme commune[858], de l'accord de coopération du 28 septembre 2006 concernant les principes pour un e-gouvernement intégré et la construction, l'utilisation et la gestion de développements et de services d'un e-gouvernement intégré[859] et, enfin, de l'accord de coopération du 26 août 2013 afin d'harmoniser et aligner les initiatives visant à réaliser un e-gouvernement intégré[860].

Ces accords de coopération fixent, en substance, des lignes directrices pour le développement de l'e-gouvernement. Les parties s'y accordent sur certains principes de base, tels que la collecte unique des données ainsi que la réutilisation maximale des informations grâce aux sources authentiques de données et à l'utilisation d'une clé d'identification unique. L'accord de 2006 consacre une disposition à la protection de la vie privée, mentionnant que les parties s'engagent à assurer l'intégrité, la sécurisation et la confidentialité des informations et à garantir le respect des lois, règlements et directives en matière de protection de la vie privée[861]. L'accord de 2013 s'inscrit également dans cette lignée, en affirmant que le respect complet des règles de protection de la vie privée et de sécurité de l'information font parties des six principes qui doivent fonder les iniatives en matière d'e-gouvernement[862].

---

[858] Accord de coopération du 23 mars 2001 entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire flamande, la Commission communautaire française et la Commission communautaire commune concernant la construction et l'exploitation d'une e-plate-forme commune, *M.B.,* 8 août 2001.

[859] Accord de coopération du 28 septembre 2006 entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire française et la Commission communautaire commune concernant les principes pour un e-gouvernement intégré et la construction, l'utilisation et la gestion de développements et de services d'un e-gouvernement intégré, *M.B.,* 19 octobre 2006.

[860] Accord de coopération du 26 août 2013 entre les administrations fédérales, régionales et communautaires afin d'harmoniser et aligner les initiatives visant à réaliser un e-gouvernement intégré, *M.B.,* 8 octobre 2013.

[861] Art. 7 de l'accord de coopération du 28 septembre 2006.

[862] Art. 3 de l'accord de coopération du 26 août 2013.

En outre, par ces accords, les parties s'engagent à créer des groupes de travail techniques. L'accord de 2001 n'en prévoit qu'un seul, alors que l'accord de 2006 crée un groupe de travail par thème ainsi qu'un comité stratégique. L'accord de 2013 affirme la possibilité de créer un groupe de travail technique et met en place un comité stratégique[863].

> Par exemple, l'article 3 de l'accord de coopération du 28 septembre 2006 prévoit la mise en place d'un groupe de travail chargé d'élaborer « des lignes d'action communes et compétences claires, concrétisées dans un plan d'approche pour l'introduction progressive du principe des sources authentiques au sein des différents niveaux de pouvoir ». Par ce groupe de travail, les parties s'engagent à « déterminer quelles données [...] sont enregistrées et mises à jour par quel service public dans leur forme authentique, et ce, le plus possible en concertation et en tenant compte des besoins de tous les autres services publics. Ce système doit ainsi permettre aux autres services publics qui ont besoin de ces données authentiques de déterminer dans quel service public ils peuvent les trouver [...] ». Un autre groupe de travail est chargé d'étudier l'introduction d'une clé d'identification unique. Un troisième groupe doit élaborer des lignes d'action communes sur le plan de la protection de la vie privée et sur le plan de la sécurité et de la traçabilité des données et des flux de données ». Un quatrième groupe doit se pencher sur l'interopérabilité tandis qu'un cinquième groupe doit veiller à « l'harmonisation de la structure de navigation et de l'offre d'informations et de services sur les sites portails des Parties ». Par ailleurs, un comité stratégique est créé, chargé d'approuver « les projets concrets réalisés » par les différents groupes de travail techniques[864].

Ces accords de coopération ont engendré maintes discussions entre les administrations fédérales, communautaires et régionales au sein des groupes de travail qui ont été constitués. On regrette, néanmoins, que ces réflexions n'aient pas toujours abouti à des avancées concrètes.

> Ainsi, en ce qui concerne l'exécution de l'accord de coopération de 2001, le groupe de travail technique, appelé *Intergovernmental Committee on E-Government (ICEG)* a été créé. Il était présidé par le gouvernement fédéral et composé de membres des administrations et des cabinets ministériels qui se sont réunis environ tous les deux mois jusqu'en 2005. Les discussions portaient sur l'échange d'informations, le financement des sources authentiques, etc. L'objectif de ce groupe était de créer une e-plateforme commune, mais il n'a pu être réalisé. Sans doute l'ambition était-elle trop grande il y a plus de dix ans. En outre, deux groupes de travail plus concrets ont été créés. Le groupe « Content » a mis au point des « lignes de vie » des citoyens pour améliorer

[863] Art. 8 et 9 de l'accord du 26 août 2013.
[864] *Ibid.*, art. 8 et 9.

la structure des portails internet. Le groupe « Architecture » était chargé de définir des standards techniques pour améliorer l'interopérabilité[865].

En ce qui concerne l'exécution de l'accord de coopération de 2006, le Comité stratégique a été créé, et constituait la continuation du groupe de travail technique de l'accord de 2001. Il a élaboré un inventaire des composants fondamentaux de l'e-gouvernement, qui n'a malheureusement jamais été publié. Il est également à l'origine du « Belgian egov community of practice »[866], une sorte de forum de discussions sur lequel on peut échanger des idées pour améliorer l'uniformisation de l'e-gouvernement en Belgique. Il est fort peu utilisé. Par ailleurs, plusieurs groupes techniques ont été formés et étaient composés uniquement de représentants des administrations. Par exemple, le groupe de travail technique relatif aux sources authentiques a été créé et s'est réuni assez régulièrement jusqu'en 2008. Il était présidé par Easi-Wal. On regrette qu'il n'ait pas dressé le tableau des sources authentiques existantes et des données s'y trouvant. Par contre, le groupe de travail relatif à l'introduction des clés d'identification uniques ne s'est jamais réuni car les parties n'en ont pas ressenti le besoin. Les thématiques semblaient déjà abordées dans les autres groupes et notamment, le groupe Sources authentiques[867].

2. Les accords de coopération impliqués par une législation sectorielle

232.- Sources authentiques et plateformes d'échanges. Il devient nécessaire d'adopter des accords de coopération concernant l'utilisation des sources authentiques et des plateformes d'échanges d'informations déjà en place. En effet, de tels outils de traitement de données imposent bien souvent des obligations à des institutions qui ne relèvent pas de l'autorité fédérale.

La section de législation du Conseil d'État s'est d'ailleurs déjà prononcée en ce sens à plusieurs reprises.

Elle a considéré qu'il était nécessaire d'adopter un accord de coopération pour rendre effective l'obligation, pour les administrations communautaires et régionales, de recourir à la collecte indirecte de données.

L'avis a ce sujet a été rendu à propos de l'article 6 de la loi sur le Registre national qui, depuis la modification de la loi en 2003, impose l'obligation de collecte indirecte des données aux autorités qui consultent cette source authentique de données. La section de législation du Conseil d'État affirme

[865] Ces standards techniques sont expliqués sur le site www.belgif.be

[866] http://www.epractice.eu/en/community/belgium

[867] Les informations relatives à la mise en œuvre des accords de coopération nous ont été fournies par le *Business Analyst* du SPF Fedict.

> que « dans la mesure où la disposition en projet [devenue l'article 6 de la loi] tend à imposer des obligations à des institutions qui ne relèvent pas de l'autorité fédérale, seul un accord de coopération conclu avec les communautés et les régions sera de nature à en assurer l'effectivité »[868].

La section de législation du Conseil d'État a également soutenu qu'un accord de coopération est nécessaire pour organiser la collecte primaire de données et leur échange entre plusieurs administrations.

> Elle s'est prononcée en ce sens concernant un avant-projet de loi organisant la collecte et l'échange de données au sein du SPF Finances. Elle a jadis invité la déléguée du ministre concerné à justifier l'avant-projet de loi « du point de vue des compétences entre l'État fédéral et les entités fédérées et à communiquer les accords existants ». Cette dernière a répondu que l'avant-projet veillait à prévenir « tout excès de compétence dans le contexte d'une Belgique fédérale. L'idée est que la collaboration nécessaire entre le SPF Finances et les administrations dépendantes des Communautés et des Régions, collaboration qui peut impliquer des transferts entre ces autorités relevant de pouvoirs distincts, s'opère dans le cadre d'accords de coopération »[869]. La section de législation du Conseil d'État a toutefois demandé que l'exposé des motifs de la loi « fournisse une liste indicative des accords existants »[870].
>
> La section de législation a adopté la même position concernant la collecte de données et l'échange de celles-ci au sein de la Banque-Carrefour des véhicules. Elle affirme que « les dispositions de l'avant-projet [...] ne pourraient [...] être comprises comme habilitant le Roi à imposer à certains services publics ou institutions relevant des communautés et des régions de participer au fonctionnement de la Banque-Carrefour en projet, notamment en ce qui concerne la collecte primaire de certaines données gérées par le réseau [...]. L'imposition de telles obligations nécessiterait, en effet, la conclusion préalable d'un accord de coopération entre les différentes entités de l'État fédéral dont relèvent les services publics et institutions concernés. Il convient, par conséquent, [...] de donner une véritable dimension 'interfédérale' au fonctionnement de la Banque-Carrefour par la conclusion préalable d'un accord de coopération si telle est l'intention de l'auteur de l'avant-projet »[871].

La Région wallonne et la Communauté française ont bien compris ces impératifs. L'accord de coopération qu'elles ont adopté le 23 mai 2013[872] s'inscrit pleinement dans le sens de ces préoccupations en organisant la

---

[868] Avis L. 33.962/2, *op. cit.,* p. 15.
[869] Avis L. 42.034/2, *op. cit.,* p. 6.
[870] *Ibid.*, p. 7.
[871] Avis L. 47.162/4, *op. cit.,* pp. 38 et 39.
[872] Accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.,* 23 juillet 2013

circulation des données entre ces deux entités fédérées. Ainsi, après avoir défini les notions clés de l'e-gouvernement[873], cet accord de coopération organise notamment la mise en place de sources authentiques de données[874] et d'une Banque-Carrefour d'échanges de données[875]. Il soumet également les administrations concernées à l'obligation de passer par la Banque-Carrefour d'échange des données pour collecter de manière indirecte les données recherchées[876].

§2. Les auteurs des accords de coopération

233.- Une confirmation par les législateurs concernés. Les accords de coopération sont librement négociés et conclus par le gouvernement fédéral et les gouvernements des entités fédérées.

Néanmoins, l'article 92*bis,* §1, alinéa 2, précise que « les accords qui portent sur les matières réglées par décret, ainsi que les accords qui pourraient grever la Communauté ou la Région ou lier des Belges individuellement, n'ont d'effet qu'après avoir reçu l'assentiment par décret. Les accords qui portent sur les matières réglées par la loi, ainsi que les accords qui pourraient grever l'État ou lier des Belges individuellement, n'ont d'effet qu'après avoir reçu l'assentiment par la loi ». Pour le dire autrement, les accords de coopération portant sur une matière qui relève de la loi, du décret ou de l'ordonnance, doivent être confirmés par les législateurs concernés. À défaut de l'être, ils ne pourront être appliqués dans l'ordre juridique de l'autorité fédérale, de la communauté ou de la région qui les a conclus[877].

De toute évidence, les accords de coopération réglant des aspects de la protection des données dans l'e-gouvernement doivent recevoir l'assentiment du législateur, et ce, en vertu de l'article 22 de la Constitution. Ce faisant, les accords de coopération sont soumis au débat démocratique et sont portés à la connaissance des citoyens, ce qui permet d'assurer, en principe, la prévisibilité de leur contenu. C'est d'ailleurs ce que la section de législation du Conseil d'État a affirmé sans détour dans son avis rendu au sujet de l'échange de données au sein du SPF Finances.

> La section de législation du Conseil d'État soutient que « comme ces accords auront une incidence sur une matière réservée à la loi, par la Constitution, et

[873] Art. 2 de l'accord de coopération du 23 mai 2013.
[874] Art. 7 et s. de l'accord de coopération du 23 mai 2013.
[875] Art. 11 et s. de l'accord de coopération du 23 mai 2013.
[876] Art. 6 de l'accord de coopération du 23 mai 2013.
[877] J Poirier, *op. cit.,* pp. 272 à 274 ; F. Delpérée, *Le droit constitutionnel de la Belgique, op. cit.*, p. 626, n° 724.

qu'ils feront varier le champ d'application de la loi à l'examen, il y aura lieu, en tout état de cause, de les soumettre à l'assentiment des assemblées législatives. Leur publication constituera une première manière de rendre prévisible l'usage des données récoltées ».

Etonnamment, les accords de coopération à vocation générale, conclus en 2001, en 2006 et en 2013, n'ont pas reçu l'assentiment des assemblées législatives. Pourtant, on peut raisonnablement soutenir qu'ils auraient dû l'être. Ils comportent, en effet, l'engagement des autorités à créer et utiliser des outils de traitement de données comme les sources authentiques de données, à instaurer l'utilisation d'une clé d'identification unique, etc. Ce sont autant de démarches qui interrogent directement la protection de la vie privée des citoyens et le principe de légalité consacré par l'article 22 de la Constitution. Ils ne pouvaient donc être laissés aux mains du seul pouvoir exécutif.

À la différence des accords de coopération à vocation générale, l'accord de coopération du 23 mai 2013 conclu entre la Région wallonne et la Communauté française a reçu l'assentiment par décret[878].

§3. La valeur des accords de coopération

234.- Valeur législative. Les accords de coopération qui ont fait l'objet d'un assentiment par une norme législative[879] ont une valeur comparable à la loi, au décret ou à l'ordonnance.

Une nuance d'importance doit néanmoins être apportée à ce propos. En effet, « les accords de coopération s'analysent comme des traités de droit interne »[880]. Qu'ils aient, ou non, reçu l'assentiment d'une norme législative, de tels accords ne peuvent être modifiés qu'avec le consentement de toutes les parties qui les ont conclus. Un partenaire ne pourrait

[878] Décret du 4 juillet 2013 portant assentiment de l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.,* 23 juillet 2013.

[879] La nature des accords de coopération n'ayant pas reçu d'assentiment législatif est une question controversée que nous ne traitons pas dans ces lignes étant donné que les accords de coopération portant sur la protection de la vie privée doivent recevoir un tel assentiment. Sur cette question, voy. M. UYTTENDAELE, *Trente leçons de droit constitutionnel, op. cit.,* pp. 850 et s.

[880] M. UYTTENDAELE, *Regards sur un système paradoxal. Précis de droit publics belge*, Bruxelles, Bruylant, 1991, p. 912.

dès lors décider de modifier unilatéralement l'accord par une norme réglementaire ou législative[881].

C'est pourquoi, d'aucuns affirment que les accords de coopération se situent, dans la hiérarchie des normes, à un niveau supérieur à celui des arrêtés royaux et de gouvernement, ou à celui des lois, décrets et ordonnances en ce qui concernent les accords de coopération ayant reçu l'assentiment d'une norme législative[882]. Plus précisément, les « accords de coopération ayant reçu un assentiment [se situent] en dessous de la loi spéciale et au-dessus des lois ordinaires, des décrets et des ordonnances »[883].

Appliquée à l'e-gouvernement, l'impossibilité, pour une autorité, de modifier unilatéralement l'accord de coopération est un atout pour l'harmonisation qui doit être réalisée en ce domaine.

On peut ainsi concevoir que le législateur fédéral construise le modèle de l'État en réseaux, organise les sources authentiques de données, les plateformes d'échanges de données, l'utilisation des numéros d'identification. Il devrait le faire dans une démarche « interfédérale », en prenant soin d'écouter les Communautés et les Régions. Au final, un ou plusieurs accord(s) de coopération pourrai(en)t être conclu(s) pour encadrer l'e-gouvernement. Etant donné que ces accords ne pourraient être modifiés unilatéralement, on peut espérer améliorer ainsi la cohérence de la matière au travers de notre État fédéral.

*

Conclusions

L'encadrement normatif de l'e-gouvernement manque de cohérence et de clarté, si bien que la protection de la vie privée des citoyens est menacée. Les deux premiers chapitres l'ont souligné à l'envi.

Ce constat convainc d'opérer une refonte substantielle de la structure administrative, de manière à protéger les données à caractère personnel des citoyens tout en ne freinant pas inutilement l'efficacité administrative. Pour ce faire, un modèle d'e-gouvernement est proposé. Il s'agit d'instituer un e-gouvernement en réseaux. Conscient des potentialités

[881] P. Coenraets, « Les accords de coopération dans la Begique fédérale », *A.P.T.*, 1992, p. 167.

[882] D. Batselé, T. Mortier et M. Scarcez, *op. cit.*, p. 467-468, n° 652 ; M. Uyttendaele, *Trente leçons de droit constitutionnel, op. cit.*, p. 853, n° 16 ; J. Vande Lanotte et G. Goedertier, *op. cit.*, p. 112, n° 192.

[883] M. Uyttendaele, *Trente leçons de droit constitutionnel*, *op. cit.*, p. 853, n° 16.

qu'offrent les technologies pour améliorer l'efficacité administrative, on encourage la circulation des données, qui facilite d'ailleurs le respect de certains principes de bonne administration. Les réseaux sectoriels, les plateformes d'échanges d'informations, les sources authentiques de données et l'utilisation de numéros d'identification rendent possible la collecte unique des données et soutiennent ainsi utilement l'efficacité de l'administration.

Néanmoins, la circulation des données pourrait mener à des dérives liberticides si elle n'était pas adéquatement encadrée. C'est pourquoi, il convient de la baliser au mieux. Appliquant la méthode du *Privacy by design,* on propose de mettre en place une structure et des outils de traitement de données qui présentent en eux-mêmes, des garanties de protection de la vie privée. L'étendue limitée des réseaux sectoriels, l'obligation de garantir la fiabilité des données enregistrées dans les sources authentiques, la possibilité, pour les plateformes d'échanges d'informations, de contrôler la proportionnalité des données échangées, ainsi que le caractère sectoriel des numéros d'identification sont autant de moyens techniques d'endiguer les abus potentiels dans les traitements de données.

Le modèle d'e-gouvernement doit ensuite être encadré par le législateur, à qui il revient d'en définir les éléments essentiels dans une loi accessible et compréhensible. C'est pourquoi, nous encourageons l'adoption de règles propres à l'e-gouvernement, qui balisent l'utilisation des outils de traitements de données et protègent les données à caractère personnel des citoyens. On suggère ainsi la rédaction de lois particulières pour encadrer chaque outil de traitement. L'adoption d'une loi-cadre pour l'e-gouvernement serait également judicieuse, pour consacrer explicitement et dans un seul texte des exigences qui, jusqu'à présent, sont disséminées dans des normes diverses, ou sont ignorées par le législateur. Enfin, ce modèle d'e-gouvernement en réseaux suppose la collaboration du législateur fédéral, des législateurs communautaires et des législateurs régionaux, puisque chaque collectivité politique détient des données qui ont vocation à être réutilisées. À cet égard, on a souligné l'intérêt d'encourager la conclusion d'accords de coopération.

*

Conclusions du Titre I

La loi est en déclin. Ce constat, dressé dans de nombreux domaines du droit, apparaît de manière évidente dans l'e-gouvernement, soumis à des normes éparses, confuses, lacunaires.

Pareille situation heurte l'article 22 de la Constitution qui protège le droit fondamental à la vie privée. Cette disposition constitutionnelle impose une exigence de légalité rigoureuse, qui confie au législateur un rôle dense. Comme l'affirment la Cour constitutionnelle et la section de législation du Conseil d'État, le pouvoir législatif est, en effet, chargé de fixer les éléments essentiels des traitements de données menés dans l'administration. Il doit le faire dans une loi claire et accessible.

Le rôle du législateur ainsi délimité doit être combiné avec le régime juridique de la protection des données à caractère personnel. Celui-ci contient des exigences qui requièrent un travail parlementaire minutieux et encouragent ainsi l'adoption de lois de qualité. En particulier, l'exigence de finalité impose au législateur de définir l'objectif du traitement de données effectué par l'administration. Il doit le faire de manière explicite, déterminée et légitime, ce qui aboutit à renforcer le principe de spécialité qui s'impose aux administrations. Par ailleurs, l'exigence de proportionnalité requiert du législateur qu'il détermine lui-même les moyens de traitements à disposition des instances administratives, ce qui lui permet de s'immiscer désormais dans des questions relevant jadis du pouvoir discrétionnaire des administrations.

Aux termes des analyses menées dans les deux premiers chapitres, on a pu affirmer que les règles de protection des données permettent au législateur de récupérer une prise sur l'action de l'administration. Ce constat est intéressant dans le contexte actuel, puisqu'il permet de contrebalancer le phénomène de déclin de la loi auquel on assiste aujourd'hui.

Il restait à savoir comment les exigences constitutionnelles et celles de la protection de la vie privée et des données à caractère personnel doivent être agencées pour encadrer adéquatement l'e-gouvernement. Le troisième chapitre répond à cette préoccupation. En analysant certains outils de traitements de données existant déjà dans l'administration belge, on s'aperçoit que la protection de la vie privée ne doit pas se réduire à quelques instruments législatifs. Cette protection peut également être assurée, en amont, par des outils qui, en eux-mêmes, présentent des garanties de fiabilité et de proportionnalité des données, notamment. Dès lors, en nous inspirant de la méthode du *Privacy by design,* on a proposé un modèle

d'e-gouvernement fondé sur ces outils de traitements de données, qui permettent un équilibre entre la protection de la vie privée des citoyens et l'efficacité administrative. Par ailleurs, on a élaboré un cadre juridique propre au secteur public, fondé sur des lois particulières et une loi-cadre, qui fixent les éléments essentiels des traitements de données effectués dans l'administration.

Les développements réalisés dans ce premier titre confirment notre hypothèse initiale. L'intégration des technologies dans l'administration ne se réduit pas à la modernisation de quelques registres de papier. Pour protéger la vie privée des citoyens qui est menacée par les progrès informatiques, il s'impose de procéder à une refonte substantielle de la structure de l'administration et d'encadrer cette structure nouvelle, comme en témoigne le modèle d'e-gouvernement en réseaux qui a été proposé dans le souci de répondre à l'article 22 de la Constitution et au régime juridique de la protection des données à caractère personnel.

* * *

Titre II.
La transparence de l'e-gouvernement

Introduction

Une exigence de transparence s'impose à l'e-gouvernement. Elle peut être définie comme l'ensemble des obligations constitutionnelles et légales qui visent à permettre au citoyen de connaître et de comprendre l'organisation et le fonctionnement de l'administration.

La transparence applicable à l'e-gouvernement se fonde sur deux corps de règles distincts. Le premier forme la transparence administrative. Le deuxième constitue la transparence des traitements de données à caractère personnel.

La *transparence administrative* permet en principe à tout administré de satisfaire sa curiosité légitime à l'égard de toutes les informations détenues par l'administration. L'objectif qui sous-tend ces règles est l'amélioration de la démocratie grâce à la connaissance et la compréhension, par chacun, de l'action administrative en général. La transparence administrative est un prolongement de l'article 10 de la Convention européenne des droits de l'homme, qui protège la liberté d'expression et d'information[884]. C'est l'idée qu'on ne peut s'exprimer pertinemment sans avoir pleinement conscience du contexte dans lequel on agit. Ce droit fondamental est consacré à l'article 32 de la Constitution, et organisé par la loi du 11 avril 1994 relative à la publicité de l'administration ainsi que plusieurs décrets ayant le même objet. Par ailleurs, la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs s'inscrit également dans le souci de transparence administrative. L'étude de ces normes fait l'objet du premier chapitre.

En vertu de la *transparence des traitements de données à caractère personnel,* tout citoyen peut, en principe, avoir connaissance des données détenues à son sujet par des tiers – en l'occurrence, il s'agit de l'administration–, et de l'utilisation qui est faite de ces informations. Cette exigence vise à assurer l'autodétermination informationnelle de toutes les personnes dont les données sont traitées. En effet, en ayant conscience que ses données sont enregistrées et utilisées au sein de l'administration, tout citoyen peut vérifier l'exactitude des informations traitées et contrôler l'usage qui en est fait. La transparence des traitements de données à caractère personnel découle de l'article 8 de la Convention européenne des droits de

[884] Voy. *infra,* n°s 240.- et s.

l'homme[885]. Elle s'impose à l'administration en vertu de l'article 22 de la Constitution et des règles de protection des données à caractère personnel à savoir, la Convention n° 108, la directive 95/46/CE et la loi du 8 décembre 1992[886]. Le deuxième chapitre y est consacré.

La présente recherche analyse les deux régimes de transparence et les confronte à l'e-gouvernement. Au regard des constats qui émergent de cette étude, on s'attèle à dégager des pistes de solutions pour enrichir ces règles et les articuler harmonieusement afin que soit effectivement garantie la transparence de l'administration dans ce contexte nouveau.

* * *

[885] Voy. not. Cour eur. D.H., *Leander c. Suède,* 26 mars 1987, req. n° 9248/81, §66 (cet arrêt concerne l'enregistrement et la communication d'informations par une autorité publique, sans possibilité pour la personne concernée d'y accéder ni de les contredire) ; *Gaskin c. RU,* 7 juillet 1989, req. n° 10454/83, §49 ; *Odièvre c. France,* 13 février 2003, req. 42326/98, §29 (ces deux derniers arrêts concernent l'accès aux informations relatives aux origines identitaires des requérants).

[886] Voy. *infra,* n°s 324.- et s.

CHAPITRE I.
L'e-gouvernement et la transparence administrative

Introduction

Longtemps dominée par le secret, l'administration a dû, progressivement, divulguer davantage d'informations au citoyen. L'émergence de la transparence administrative est marquée par la consécration d'un droit fondamental dans la Constitution ainsi que l'adoption de plusieurs normes légales. Aujourd'hui, le citoyen se voit reconnaître le droit de savoir comment est structurée l'administration et comment elle fonctionne. Il a également le droit de comprendre l'action administrative.

L'idéal de transparence poursuivi par cet arsenal normatif est aujourd'hui ébranlé par le développement de l'e-gouvernement. Dans quelle mesure le citoyen peut-il encore satisfaire sa soif de connaissance et de compréhension dans l'environnement administratif qui l'entoure à l'heure du déploiement des technologies au sein de l'administration ?

*

Section 1. La notion de transparence administrative

235.- Définition. La transparence administrative vise l'ensemble des normes qui organisent la publicité des documents de l'administration et la motivation formelle des actes administratifs. Elle est aujourd'hui érigée en droit fondamental à l'article 32 de la Constitution et organisée par diverses législations. Cet arsenal normatif est l'aboutissement d'une remise en cause progressive et fondamentale de la relation entre l'administration et les administrés. Les lignes qui suivent y sont consacrées.

I. L'émergence de la transparence administrative

236.- Considérations générales. Les normes qui organisent la transparence administrative ont progressivement été adoptées en réaction au secret qui a longtemps entouré l'administration.

La transparence administrative est justifiée aujourd'hui par la volonté d'améliorer le fonctionnement de la démocratie. Elle offre des moyens qui contribuent à placer l'administration et le citoyen sur un pied d'égalité, afin d'en faire des collaborateurs qui ne se cachent rien, plutôt que des adversaires qui nourrissent une méfiance mutuelle. Ces règles sont donc particulièrement importantes dans le contexte de l'e-gouvernement. Rappelons[887], en effet, que l'intégration des technologies dans l'administration ébranle l'équilibre entre l'administration et les citoyens en raison du fait, notamment, que les traitements de données réalisés par l'État sont bien souvent opaques.

A. L'origine de la transparence administrative

237.- Une administration longtemps secrète. Dans l'Ancien Régime, et durant des années ensuite, l'administration fonctionne de manière fermée et secrète[888]. Elle apparaît comme « une administration de souveraineté et de commandement, hiérarchisée et centralisée à l'extrême, aux décisions de type militaire, unilatérales, impératives, contraignantes, fondées sur l'assujettissement de l'individu à la puissance publique et à ses prérogatives : une administration qui interdit, ordonne, réglemente, accorde ou refuse ses bienfaits, sans rendre compte aux administrés »[889]. Dans ce contexte, le citoyen est considéré comme un subordonné, tenu à l'écart de l'action administrative[890]. Les seules relations qui s'établissent entre l'administration et les administrés le sont exclusivement au bénéfice de la première. Elles s'expliquent par le besoin de l'administration d'obtenir les informations nécessaires pour l'accomplissement de ses missions ou d'imposer des prescriptions administratives. L'administration de l'époque se marque donc par son « emprise [...] sur une société censée être 'transparente' à elle, malléable et docile. [...] Dépourvus de la moindre prise sur les processus administratifs qui se déroulent hors de leur portée

[887] Voy. *supra* n°s 46.-et s.

[888] Projet de loi relatif à la publicité de l'administration, *Doc. Parl.,* Ch. Repr., sess. 1992-1993, n° 1112/1, p. 2.

[889] J. Lemasurier, « Vers une démocratie administrative : du refus d'informer ou droit d'être informé », *Revue de droit public et de la science politique en France et à l'étranger,* 1980, p. 1239.

[890] Projet de loi relatif à la publicité de l'administration, Rapport fait au nom de la commission de l'intérieur, des affaires générales et de la fonction publique par L. Peeters, *Doc. Parl.,* Ch. Repr., sess. 1993-1994, n° 1112/13, p. 11.

et de leur regard, les administrés sont invités à s'en remettre à l'infinie sagesse administrative »[891].

238.- Une insatisfaction généralisée. L'organisation traditionnelle de l'administration provoque l'insatisfaction de tous.

Pour le parlementaire, le pouvoir grandissant de l'administration est une limitation de son mandat, et ce d'autant plus qu'il ne peut qu'insuffisamment contrôler l'appareil bureaucratique[892].

Le citoyen est frustré par le secret derrière lequel se retranche l'administration. Il peine à comprendre la structure complexe de cette bureaucratie fermée sur elle-même et impersonnelle. Plus encore, il se sent désarmé face aux refus que lui oppose l'administration lorsqu'il pose une question ou souhaite accéder à un document administratif[893].

Enfin, le fonctionnaire est mal à l'aise, étant tenu de subir la méfiance que les hommes politiques et les citoyens manifestent à l'égard de l'administration[894]. Le secret apparaît de plus en plus comme un obstacle à la légitimité de l'action administrative.

239.- Le besoin d'une nouvelle relation administration-administrés. Partant de l'insatisfaction généralisée provoquée par l'opacité et la distance de l'administration, la nécessité s'impose progressivement de repenser le fonctionnement de celle-ci, et, en particulier, d'améliorer substantiellement la relation entre l'administration et les administrés. On affirme ainsi l'urgence de placer le citoyen au centre de l'organisation et du fonctionnement de l'appareil administratif[895]. L'administration de décision doit devenir une administration de dialogue, accessible et conviviale[896].

C'est dans ce contexte qu'est adoptée, le 4 décembre 1992, la Charte de l'utilisateur des services publics[897], qui n'est pas « une simple déclaration d'intention » mais bien « une véritable directive de fonctionnement que le Gouvernement entend imposer aux services publics »[898]. Ce texte pose

---

[891] J. CHEVALLIER, « Le mythe de la transparence administrative », *Information et transparence administratives,* Paris, PUF, 1988, p. 252.

[892] Projet de loi relatif à la publicité de l'administration, Exposé des motifs, *op. cit.*, p.4.

[893] *Idem.*

[894] *Idem.*

[895] *Idem.*

[896] Proposition de loi relative à la motivation formelle des actes administratifs, Rapport fait au nom de la Commission de l'intérieur par M. Flagothier, *Doc. Parl.,* Sénat, sess. 1990-1991, p. 10.

[897] Charte de l'utilisateur des services publics du 4 décembre 1992, *M.B.,* 22 janvier 1993.

[898] Préambule de la Charte de l'utilisateur des services publics.

des principes généraux et définit des mesures concrètes pour « procurer un service public adapté aux besoins de chaque utilisateur ».[899] Parmi ces principes et ces mesures, figure la transparence des services publics.

> Soulignons que, pour satisfaire l'objectif de transparence, la Charte impose notamment aux services publics le devoir de « vulgariser par tous les vecteurs de communication adéquats les axes majeurs de leur politique, de prendre des initiatives en vue d'informer les utilisateurs sur les services qu'ils offrent et de donner accès à l'utilisateur à l'information qui a trait à sa personne »[900]. Cette exigence est intéressante s'agissant de la transparence des traitements de données à caractère personnel. Nous y reviendrons[901].

B. La raison d'être de la transparence administrative

240.- L'article 10 de la Convention européenne des droits de l'homme. L'administration doit être réorganisée en vue d'instaurer une relation plus équilibrée entre les pouvoirs publics et le citoyen. Pour ce faire, il s'impose de créer des puits de lumière dans la forteresse administrative en garantissant au citoyen un « droit à l'information », c'est-à-dire le « droit de disposer de toutes les informations indispensables pour donner une signification à la notion 'un état de droit démocratique' »[902].

La transparence administrative s'inscrit dans le prolongement du droit fondamental à la liberté d'expression consacré à l'article 10 de la Convention européenne des droits de l'homme. Par souci de clarté, rappelons que l'article 10 de la Convention européenne des droits de l'homme prévoit, en son premier paragraphe, que « toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière »[903].

Bien que la Cour européenne des droits de l'homme n'ait jamais reconnu explicitement que l'article 10 de la Convention européenne des droits de l'homme consacre un droit d'accès général aux documents administratifs

---

899 *Idem*.

900 Partie I, Chapitre 1er. de la Charte de l'utilisateur des services publics.

901 Voy. *infra* n° 381.-

902 Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Note explicative, *Doc. Parl.*, Ch. repr., session 1992-1993, n° 839/1, p. 1.

903 C'est nous qui soulignons.

détenus par les autorités publiques[904], depuis plusieurs années, elle donne à la notion de « liberté de recevoir des informations » une interprétation de plus en plus large, qui se rapproche d'un droit d'accès à l'information[905]. En outre, la jurisprudence de la Commission européenne des droits de l'homme[906], nombre de résolutions et recommandations du Conseil de l'Europe[907], ainsi que la doctrine[908], mettent en évidence l'existence d'un lien direct entre la transparence administrative et le droit fondamental à la liberté d'expression. Ce lien a encore été affirmé par le gouvernement lors des discussions préalables à l'adoption, dans notre Constitution, du droit fondamental à la transparence administrative[909]. C'est l'idée que si le citoyen n'a pas connaissance des informations utilisées par les autorités publiques, il n'est pas à même de s'exprimer justement à propos du fonctionnement de l'État et de prendre part pleinement au débat démocratique. Plus particulièrement, la transparence administrative constitue, pour le citoyen, un instrument de connaissance et de participation démo-

[904] À ce sujet, voy. not. D. Voorhoof, « Artikel 10 – Vrijheid van meningsuiting », *in Handboek EVRM* (dir. J. Vande Lanotte et Y. Haeck), partie 2, *Artikelsgewijze commentaar,* vol. 1, Anvers, Intersentia, 2004, pp. 913 et s. ; F. Sudre, « Les aléas de la notion de 'vie privée' dans la jurisprudence de la Cour européenne des drtois de l'homme », *in Mélanges en hommage à Louis Edmond Pettiti,* Bruxelles, Bruylant, 1998, pp. 704 et s. ; D. Deom, T. Bombois et L. Gallez, « Les exceptions au droit d'accès aux documents administratifs », *in L'accès aux documents administratifs* (dir. D. Renders), Bruxelles, Bruylant, 2008, pp. 233 et s.

[905] À cet égard, voy. C.E.D.H., déc. *Sdružení Jihočeské Matky c. République tchèque*, 10 juillet 2006, req. 19101/03 ; C.E.D.H., arrêt *Tarsasag c. Hongrie*, du 14 avril 2009, req. 37374/05.

[906] Comm. eur. D.H., arrêt *Finegan c. Irlande,* du 7 décembre 1981, req. 8878/80, *in*édite ; arrêt *X. c. République fédérale d'Allemagne,* du 3 octobre 1979, req. 8383/78, *Decisions and Reports* 17, 228 ; arrêt *X. c. Autriche,* du 13 avril 1988, req. 10392/83, *in*édite, cités par C. de terwangne, « Le droit à la transparence administrative », *in Les droits fondamentaux dans la Constitution belge* (dir. M. Verdussen et N. Bonbled), Bruxelles, Bruylant, 2011, p. 708.

[907] Résolution 428 (1970) portant déclaration sur les moyens de communication de masse et les droits de l'homme ; Recommandation 582 (1970) relative aux moyens de communication de masse et droits de l'homme ; Recommandation 854 (1979) relative à l'accès du public aux documents gouvernementaux et à la liberté d'information ; Recommandation 1037 (1986) relative à la protection des données et à la liberté d'information.

[908] C. de Terwangne, *Société de l'information et mission publique d'information,* Thèse de doctorat, Namur, FUNDP, 2000, n° 44-133 http://www.crid.be/pdf/public/These_cdeterwangne.pdf ; C. de Terwangne, « La Convention européenne des droits de l'homme et le droit de recevoir des informations de la part des autorités publiques », *Amén.- Env.,* 1998, pp. 265-267 ; P. Lewalle, L. Donnay et G. Rosoux, « L'accès aux documents administratifs, un itinéraire sinueux », *L'accès aux documents administratif* (dir. D. Renders), Bruxelles, Bruylant, 2008, pp. 43-46.

[909] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Note explicative, *Doc. Parl.,* Ch. repr., session 1992-1993, n° 839/1, pp. 1-4.

cratique ainsi qu'un instrument de contrôle. Pour l'administration, elle est un instrument de rapprochement et d'efficacité.

241.- Un instrument de connaissance et de participation démocratique. La transparence offre aux citoyens « la possibilité d'agir en connaissance de cause »[910]. En effet, en accédant à l'information détenue par l'administration, les citoyens peuvent prendre connaissance des politiques menées ou en voie de l'être. Ils sont à même de se forger un avis, d'évaluer les décisions adoptées pour ensuite y adhérer, ou non. Ils ont une prise sur l'administration et peuvent exiger d'elle qu'elle rende des comptes, qu'elle justifie les choix posés et les rectifie éventuellement.

La transparence offre donc aux citoyens une place dans le processus décisionnel. Ils peuvent prendre part au débat public en pleine connaissance de cause. La publicité de l'administration contribue ainsi à la mise en œuvre effective de la démocratie[911].

242.- Un instrument de contrôle. La transparence de l'administration soumet celle-ci au regard du public et à son éventuelle contestation. Des recours contre les décisions prises ne seront pas nécessairement effectués, mais ils relèvent de l'ordre du possible.

Cette possibilité de contrôle effectif pousse l'administration à se soucier de la légalité de son action. Cela peut modifier les processus de décision, les conditions d'exercice de l'autorité hiérarchique, les rapports internes, etc. Ainsi peut-on soutenir que « la transparence se présente à la fois comme le moyen de lutte par excellence contre la corruption, les abus et les détournements de pouvoirs, et comme le rempart contre le gaspillage des deniers publics »[912].

---

[910] G. Braibant, « Droit d'accès et droit à l'information », *in Service public et libertés. Mélanges offerts au professeur Robert-Edouard Charlier,* Paris, Éd. de l'Université et de l'Enseignement moderne, 1981, p. 704.

[911] R. Ergec, « La transparence administrative comme droit fondamental et ses limites », *A.P.T.,* 1993, p. 87 ; C. de Terwangne, *Société de l'information et mission publique d'information,* n° 14 et références citées ; F. Jongen, « La publicité de l'administration », *op. cit.,* p. 777 ; J. Chevallier, « Le mythe de la transparence administrative », *op. cit.,* pp. 244 et 254 ; G. Braibant, « Réflexions sur les perspectives d'évolution de l'administration », *R.F.A.P.,* 1979, p. 181 ; P. De Hert, « De grondrechten en wetten m.b.t. openbaarheid van bestuursdcument en bescherming van persoonlijke levensfeer. Analyse van de onderlinge relatie en commentaar bij het arrest Dewinter van de Raad van State », *C.D.P.K.,* 2001, pp. 390 et 391 ; D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *Droit administratif. Tome III. Le contrôle de l'administration,* Bruxelles, Larcier, 2010, p. 69.

[912] C. de Terwangne, *Société de l'information et mission publique d'information, op. cit.,* n° 17. Voy. égal. E. Brems, « De nieuwe grondrechten in de Belgische Grondwet en hun verhouding tot het Internationale, *in*zonderheid het Europese Recht », *T.B.P.,* 1995, p. 621 ;

243.- Un instrument de rapprochement et d'efficacité. Plus l'administration est opaque, plus elle risque d'être omnipotente. La difficulté d'en cerner les contours génère donc de la méfiance auprès des citoyens et affaiblit la légitimité des actes de l'administration[913]. Inversement, la transparence incite l'administration et le citoyen à engager un dialogue. Cette voie rapproche les deux partenaires autour des mêmes problématiques administratives et génère des rapports humains personnalisés. À la logique de l'unilatéralité succède celle du dialogue.

La transparence apparaît donc comme un instrument de rapprochement entre l'administration et les administrés, en « rendant les frontières entre l'administration et la société, non plus étanches mais poreuses : des liens vont être tissés, des passerelles lancées, qui réduisent l'opacité administrative, rendent plus ténue l'enveloppe formelle de l'organisation et rendent l'administration sensible à son environnement social »[914]. Grâce à la proximité établie et le dialogue engendré, les citoyens comprennent davantage les politiques menées et y consentent avec moins de méfiance. Un tel consensus est nécessaire à l'administration pour accomplir ses tâches. Il sous-tend ainsi l'efficacité de l'action publique[915].

> C'est d'ailleurs ce que souligne la Charte de l'utilisation des services publics, qui présente la transparence comme un moyen d' « augmenter la confiance que les utilisateurs placent [dans les services publics], ce qui renforcera finalement l'efficacité »[916].

II. Le contenu de la transparence administrative

244.- Une maison de verre. De manière métaphorique, l'administration transparente est décrite comme une maison de verre au sein de laquelle les agents travaillent sous le regard des citoyens, sont disponibles pour répondre à leurs questions dans un langage intelligible et leur

---

F. Schram, « Openbaarheid van bestuur en de burgelijke stand », *T.B.P.*, 1998, pp. 391-397 ; J. Chevallier, « Le mythe de la transparence administrative », *op. cit.,* p. 255 ; R. Ergec, « La transparence administrative comme droit fondamental et ses limites », *op. cit.,* p. 88 ; P. De Hert, « De grondrechten en wetten m.b.t. openbaarheid van bestuursdcument en bescherming van persoonlijke levensfeer. Analyse van de onderlinge relatie en commentaar bij het arrest Dewinter van de Raad van State », *op. cit.*, pp. 390 et 391 ; D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.*, pp. 69 et 70.

[913] Projet de loi relatif à la publicité de l'administration, Exposé des motifs, *op. cit.*, p.4.

[914] J. Chevallier, « Le mythe de la transparence administrative », *op. cit.,* p. 255.

[915] Ibid., p. 256 ; C. de Terwangne, *Société de l'information et mission publique d'information*, *op. cit.*, n° 18.

[916] Charte de l'utilisateur du service public du 4 décembre 1992, chapitre 1.

présenter les documents qu'ils souhaitent consulter[917]. Il s'agit d'un idéal dans la perspective duquel s'inscrivent les normes organisant la transparence administrative.

Parmi ces normes, certaines visent à garantir au citoyen un *droit de savoir*. L'article 32 de la Constitution et la loi du 11 avril 1994 relative à la publicité de l'administration[918], tout comme les décrets ayant le même objet, répondent à cette préoccupation.

Par ailleurs, le citoyen se voit également reconnaître un *droit de comprendre*. La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs[919] s'inscrit dans cette perspective.

Certes, la division « droit de savoir » et « droit de comprendre » est assez catégorique. Toutefois, il y est recouru pour la clarté de l'exposé qui est consacré, dans un premier temps, à la publicité de l'administration via l'accès aux documents administratifs et, dans un deuxième temps, à la motivation formelle des actes administratifs. Le droit de savoir est donc utilisé pour la transparence de l'administration en général, tandis que le droit de comprendre vise la motivation des décisions administratives en particulier. Néanmoins, droit de savoir et droit de comprendre sont étroitement liés. Le droit de « savoir » comprend également un droit de comprendre : nous verrons en effet que le citoyen dispose du droit d'obtenir des explications, qui est un corollaire du droit d'accès aux documents administratifs. Dans le même sens, le droit de comprendre les décisions administratives individuelles suppose bien sûr qu'on les connaisse.

A. Le droit de savoir : la publicité des documents administratifs

245.- Le droit de savoir. La transparence de l'administration suppose que tout citoyen puisse avoir connaissance de l'administration dans son ensemble. Il a ainsi le droit de savoir comment est structurée l'administration et comment elle fonctionne. En outre, toute personne doit pouvoir accéder à son dossier en particulier. Il a le droit de savoir ce que les autorités administratives détiennent à son sujet. Il doit pouvoir rectifier les éventuelles informations erronées. Il doit avoir la possibilité de communiquer des informations complémentaires[920].

---

[917] R. Andersen, « Conclusions de la journée d'études sur les communes et la transparence administrative », *Rev. Dr. Comm.*, 1999, p. 127.

[918] Loi du 11 avril 1994 relative à la publicité de l'administration, *M.B.*, 30 juin 1994.

[919] Loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs, *M.B.*, 12 septembre 1991.

[920] F. Delpérée, « Le droit constitutionnel et la transparence », *L'accès aux documents administratifs* (dir. D. Renders), Bruxelles, Bruylant, 2008, p. 16.

Le droit de savoir s'ancre aujourd'hui dans l'article 32 de la Constitution et dans les législations relatives à la publicité de l'administration. Les lignes qui suivent en dressent un panorama général. Ces normes organisent la publicité passive de l'administration, c'est-à-dire la diffusion de l'information à la demande du citoyen. Elles prévoient également des obligations de publicité active de manière à ce que les autorités publiques divulguent des informations de leur propre initiative. La publicité passive et la publicité active de l'administration sont étudiées dans la section 2, au regard de l'e-gouvernement.

246.- L'article 32 de la Constitution : le droit fondamental à la publicité des documents administratifs. Le 18 juin 1993, la Constitution s'enrichit d'un droit fondamental nouveau. Il est consacré à l'article 24 *ter*, devenu, depuis lors, l'article 32 de la Constitution coordonnée. Selon cette disposition, « chacun a le droit de consulter tout document administratif et de s'en faire remettre copie, sauf dans les cas et conditions fixés par la loi, le décret ou la règle fixée à l'article 134 de la Constitution ». Le droit à la publicité des documents administratifs est ainsi érigé au rang de droit fondamental.

La consécration du droit fondamental d'accéder aux documents administratifs constitue à l'époque une véritable révolution pour l'action administrative qui, rappelons-le, était jusque là dominée par le secret. Rares étaient les documents administratifs bénéficiant d'une publicité organisée par des législations particulières[921]. L'article 32 de la Constitution vint inverser cette logique. Il fit de la transparence la règle et du secret, l'exception, en s'inscrivant directement dans le prolongement de l'article 10 de la Convention européenne des droits de l'homme, comme cela a été dit précédemment.

247.- Un renvoi vers les législateurs. L'article 32 de la Constitution est volontairement succinct, à l'image des autres droits fondamentaux

[921] Il faut tout de même noter que quelques législations particulières organisaient déjà la publicité de certains documents administratifs tels que les délibérations des organes communaux et provinciaux, les listes des électeurs, les documents officiels du cadastre, les informations relatives à l'environnement, les dossiers et documents relatifs aux procédures ouvertes aux citoyens (enquêtes publiques, expropriations pour cause d'utilité publique, urbanisme et aménagement du territoire, etc). Voy. C. Benedek, « La transparence administrative en Belgique. L'accès aux documents administratifs », *A.P.T.*, 1993, pp. 162 et 163 ; C. de Terwangne, « Le droit à la transparence administrative », *op. cit.*, p. 705 ; Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Rapport fait au nom de la Commission de la révision de la Constitution, des Réformes institutionnelles et du règlement des conflits par M. Reynders, *Doc. Parl.*, Ch. repr., sess. 1992-1993, n° 839/4, p. 2.

repris dans la Constitution. Comme affirmé lors des discussions préparatoires, cette disposition « fixe les principes de base concernant la publicité de l'administration. Il est opté pour une brève définition de ces principes. Une spécification plus détaillée ne peut que prêter à confusion [...]. Le danger est trop grand que ce qui n'est pas repris soit interprété comme une restriction volontaire ou involontaire »[922].

Le Constituant a laissé au législateur fédéral et aux législateurs communautaires et régionaux, le soin d'organiser la mise en œuvre du droit d'accès aux documents administratifs et de fixer éventuellement des exceptions à celui-ci, dans les matières qui ressortissent à leurs compétences[923]. C'est la raison pour laquelle l'article 32 de la Constitution tempère le caractère catégorique du droit fondamental en précisant « sauf dans les cas et conditions fixés par la loi, le décret ou la règle visée à l'article 134 ». Afin de leur laisser le temps d'intervenir, une disposition transitoire a été adoptée, fixant l'entrée en vigueur du droit fondamental au 1er janvier 1995[924]. C'est ainsi que, progressivement, la publicité de l'administration s'est déployée au travers de plusieurs législations.

248.- Une législation plurielle. Le droit à la publicité des documents administratifs est organisé par les différents législateurs du pays, comme les y invite l'article 32 de la Constitution.

Le législateur fédéral était déjà à l'œuvre au moment de la révision constitutionnelle. Un projet de loi était en effet déposé devant la Chambre des représentants[925]. Il devint la loi du 11 avril 1994 relative à la publicité de l'administration.

Les législateurs des entités fédérées ont suivi le pas. De manière générale, la loi du 11 avril 1994 leur a servi de modèle, bien que des divergences n'aient pu être évitées. Ainsi, la Communauté française a adopté,

---

[922] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Note explicative, *op.cit.*, n° 839/1, p. 4.

[923] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Rapport fait au nom de la Commission de la révision de la Constitution, des Réformes institutionnelles et du règlement des conflits par M. Reynders, *op. cit.,* n° 839/4, p. 2.

[924] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Rapport fait au nom de la Commission de la révision de la Constitution, des Réformes institutionnelles et du règlement des conflits par M. Reynders, *op. cit.,* n° 839/4, p. 3. Le ministre a souligné qu'un délai devait être fixé pour « exercer une certaine pression sur les autorités tant législatives qu'exécutives » (Rapport fait au nom de la commission de la révision de la Constitution et des réformes des institutions, *op. cit.*, n° 100-49/2°, p. 9).

[925] Projet de loi relatif à la publicité de l'administration, *Doc. Parl.,* Ch. Repr., sess. 1992-1993, n° 1112/1.

le 22 décembre 1994, un décret relatif à la publicité de l'administration[926]. Le 30 mars 1995, la Région de Bruxelles-Capitale et la Région wallonne ont fait de même.

L'intervention des autres législateurs s'est faite attendre, dépassant le délai du 1er janvier 1995. La Communauté germanophone s'est dotée d'un décret relatif à la publicité des documents administratifs le 16 octobre 1995. Suivirent la Commission communautaire française, le 11 juillet 1996 et la Commission communautaire commune, le 26 juin 1997. Finalement, le 12 novembre 1997, le législateur organisa la publicité de l'administration dans les provinces et les communes[927]. En Flandre, la publicité de l'administration était déjà organisée deux ans avant le vote de l'article 32 de la Constitution. Mais le 18 mai 1999, ce premier décret fut abrogé et remplacé par un décret relatif à la publicité de l'administration, qui fut lui-même remplacé par un décret du 26 mars 2004[928].

249.- Une législation embroussaillée. Le plus souvent, les législateurs des entités fédérées se sont largement inspirés des règles prévues par la loi du 11 avril 1994. Il n'en demeure pas moins que ces interventions législatives multiples ont généré une législation embroussaillée, composée de textes semblables sans être identiques pour autant. D'aucuns soutiennent ainsi que la législation sur la transparence « manque elle-même de transparence »[929].

B. Le droit de comprendre : la motivation formelle des actes administratifs

250.- Le droit de comprendre. La transparence administrative ne pourrait se réduire à la publicité des documents détenus par les autorités administratives. Il faut également donner aux citoyens les moyens de comprendre les décisions prises, de « reconstituer la démarche intellectuelle des autorités publiques [...], comprendre l'alchimie d'un processus souvent complexe de décision »[930]. C'est dans cette perspective qu'a été adoptée la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs.

---

[926] *M.B.*, 31 décembre 1994.

[927] Loi du 12 novembre 1997 relative à la publicité de l'administration dans les provinces et les communes, *M.B.*, 19 décembre 1997.

[928] Décret du 26 mars 2004 relatif à la publicité de l'administration, *M.B.*, 1er juillet 2004.

[929] P. Lewalle, L. Donnay et G. Rosoux, « L'accès aux documents administratifs, un itinéraire sinueux », *L'accès aux documents administratifs, op. cit.*, p. 28.

[930] F. Delpérée, « Le droit constitutionnel et la transparence », *op. cit.*, p. 17.

251.- La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs[931]**.** À l'instar de l'article 32 de la Constitution et des différentes législations en matière d'accès aux documents administratifs, la loi du 29 juillet 1991 s'inscrit dans le mouvement de renouveau administratif, qui opère le basculement du principe du secret vers celui de la transparence. Cette loi, qui sera étudiée plus loin[932], impose aux autorités administratives de motiver, en droit et en fait, les actes administratifs qu'elles adoptent. De cette manière, les personnes concernées peuvent comprendre les raisons qui ont conduit l'autorité à prendre une décision en leur faveur ou à leur détriment. Elles sont également éclairées quant au fait que les décisions prises ne sont pas arbitraires et ont été élaborées de manière rigoureuse. Plus encore, en cas de contestation de la décision, l'inscription des motifs dans l'acte lui-même permet à l'administré de mieux organiser ses moyens[933]. Cela facilite également le travail des autorités de contrôle « qui ne doivent plus partir à la recherche des motifs dans les méandres du dossier administratif »[934].

Section 2. Le droit de savoir ébranlé par l'e-gouvernement

252.- Publicité passive et publicité active. La publicité de l'administration telle qu'organisée aujourd'hui, comporte deux volets que sont la publicité passive et la publicité active.

La publicité passive vise l'information diffusée à la demande du citoyen. La publicité est dite « passive » car on se place dans le chef de l'administration. Celle-ci n'est tenue qu'à une obligation de publicité passive puisqu'il lui revient seulement de donner suite aux demandes qui lui sont adressées d'initiative par les citoyens[935]. Elle n'a pas d'obligations actives

---

[931] Loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs, *M.B.,* 12 septembre 1991.

[932] Voy. *infra,* n°s 313.- et s.

[933] Proposition de loi relative à la motivation formelle des actes administratifs, Développements, *Doc. Parl.,* Sénat, sess. extr. 1988, n° 215-1, p. 1.

[934] X. Delgrange et B. Lombaert, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : questions d'actualité », *in La motivation formelle des actes administratifs* (dir. P. Jadoul et S. Van Drooghenbroeck), Bruxelles, La Charte, 2005, p. 5, n° 4.

[935] Voy. entre autres nombreux auteurs, C. Hoorevoets, « Article 32 », *in La Constitution belge. Lignes et entrelignes* (dir. M. Verdussen), *op. cit.,* p. 119 ; R. Andersen, « La mise en balance des intérêts en cause dans l'appréciation des motifs d'exception à la publicité de l'administration », *op. cit.*, p. 38 ; P. Bouvier, *Éléments de droit administratif,* Bruxelles, De Boeck, 2002, p. 219.

en ce sens qu'elle n'est pas contrainte de rassembler et de diffuser, d'initiative, des informations sur leurs activités[936].

À l'inverse, *la publicité active* vise l'information diffusée à l'initiative de l'administration, sans attendre la demande d'un administré.

Jusqu'à présent, c'est la publicité passive qui a principalement retenu l'attention du constituant et du législateur. L'article 32 de la Constitution vise exclusivement la publicité passive puisqu'elle protège le droit d'accès et de communication des documents administratifs. Quant à la loi du 11 avril 1994, elle consacre la majorité de ses dispositions à la publicité passive, qui est ainsi réglementée de manière bien plus détaillée que la publicité active.

La suite de la recherche n'entend pas recenser et analyser chaque aspect de chacune de ces normes. Il s'agit plutôt de les aborder au travers du prisme de l'e-gouvernement, afin de souligner les forces et les faiblesses de cette législation lorsqu'elle est confrontée à l'usage des technologies. Cette analyse est effectuée principalement au regard de l'article 32 de la Constitution et de la loi du 11 avril 1994 puisque cette dernière a servi de modèle aux législateurs des entités fédérées. Néanmoins, nous soulignons les particularités de certaines normes communautaires ou régionales lorsque celles-ci présentent un intérêt particulier.

Compte tenu de sa place importante dans l'arsenal normatif, la publicité passive de l'administration est étudiée dans un premier temps. Dans un deuxième temps, la recherche se consacre à la publicité active des informations administratives.

I. La publicité passive confrontée à l'e-gouvernement

253.- Une garantie légale ébranlée par les TIC. Le droit de tout citoyen à la publicité passive des documents administratifs est affirmé à l'article 4 de la loi du 11 avril 1994 en ces termes :

« Le droit de consulter un document administratif d'une autorité administrative fédérale et de recevoir une copie du document consiste

[936] Remarquons que, lors des discussions qui ont précédé l'adoption de la loi du 11 avril 1994 relative à la publicité de l'administration, laquelle consacre les notions de « publicité active » et de « publicité passive », un membre de la Commission de l'Intérieur a très pertinemment souligné qu « 'actif' et 'passif' étant des données relatives selon que l'on se place du poins de vue de celui qui agit ou qui subit, on doit s'étonner qu'une loi mettant en œuvre un droit reconnu au citoyen, et non pas à l'administration, adopte le point de vue de l'administration ». (Projet de loi relatif à la publicité de l'administration, Rapport fait au nom de la Commission de l'intérieur, des Affaires générales et de la Fonction publique, *Doc. Parl.,* Ch. repr., sess. 1993-1994, n° 112/12, p. 7).

en ce que chacun, selon les conditions prévues par la présente loi, peut prendre connaissance sur place de tout document administratif, obtenir des explications à son sujet et en recevoir communication sous forme de copie ».

Il s'impose, dans ce chapitre, d'évaluer cette garantie au regard des développements récents de l'administration à l'heure de l'électronique. Comme cela a été abondamment souligné dans le premier titre de cette recherche, grâce à la mise en œuvre de la collecte unique des données les compétences de l'administration sont, de plus en plus souvent, accomplies sans importuner le citoyen. Pour autant, le citoyen ne se désintéresse pas de la chose publique. Au contraire. Même si l'usage de l'informatique dans l'administration présente maints avantages et génère ainsi de l'enthousiasme, il crée également certaines appréhensions. Nombre de personnes craignent la perte de la maîtrise de leurs informations ainsi que le développement d'une administration entièrement automatisée qui, froide et distante, réduirait les personnes à un numéro d'identification.

Il importe dès lors, aujourd'hui plus encore qu'hier, de veiller à garantir aux citoyens un accès aisé aux documents administratifs, dans le but de répondre aux trois impératifs qui fondent la transparence et qui ont précédemment été mis en évidence, à savoir, la participation citoyenne, le contrôle de l'action administrative, et la confiance en l'administration. Pourtant, à l'heure actuelle, le citoyen désireux d'accéder aux documents administratifs relatifs à l'e-gouvernement est confronté à des questions et des embûches. Dans ce contexte, la transparence administrative est-elle effective ?

La structure des développements qui suivent est calquée sur le parcours que doit suivre un citoyen pour accéder à un document. Ainsi, dans un premier temps, on porte attention à la demande d'accès au document recherché avant de se pencher, dans un deuxième temps, sur la réponse de l'autorité qui détient le document.

A. La demande d'accès

254.- L'article 5 de la loi du 11 avril 1994. En vertu de l'article 5 de la loi du 11 avril 1994, « la consultation d'un document administratif, les explications y relatives ou sa communication sous forme de copie ont lieu sur demande. La demande indique clairement la matière concernée, et, si possible, les documents administratifs concernés, et est adressée par écrit à l'autorité administrative fédérale compétente, même si celle-ci a déposé le document aux archives ».

Les lignes qui suivent étudient la forme, la formulation et l'objet de la demande au regard de certains développements de l'e-gouvernement.

§1. La forme de la demande

255.- Un « écrit ». Adoptée à l'ère du papier, la loi indique, sans surprise, que la demande d'accès doit être formulée par écrit.

L'électronique envahissant progressivement les rapports entre l'administration et les administrés, la question se pose naturellement de savoir si le terme « écrit » suppose, encore aujourd'hui, l'utilisation de papier. Pour le dire autrement, le citoyen peut-il introduire une demande d'accès par un courriel ou un fax plutôt que par une lettre en papier ? La réponse varie selon que le législateur a répondu explicitement à cette question, ou non.

256.- Première hypothèse : le législateur est explicite. Lorsque le législateur prévoit explicitement l'utilisation du courriel ou du fax, les demandes introduites sous ces formes sont évidemment recevables.

Le législateur flamand a pensé à l'usage des technologies lorsqu'il a révisé son décret sur la publicité de l'administration en 2004. Il a assimilé explicitement le courriel et le fax à un écrit traditionnel.

> Ainsi, à l'article 17, §1, du décret flamand du 26 mars 2004 relatif à la publicité de l'administration[937] est-il prévu que « la demande est présentée par écrit. Par demande écrite, on entend une demande introduite par lettre, par fax, par e-mail ou remise en main propre [...] ».

257.- Deuxième hypothèse : le législateur est silencieux. Que faire si la loi ne prévoit rien explicitement, comme c'est le cas de la loi du 11 avril 1994 ? La réponse ne s'impose pas de manière évidente.

a) La prudence. Dans l'attente de solutions légales explicites, David De Roy invite à la prudence en soutenant qu'on ne peut pas nécessairement assimiler un écrit traditionnel à un écrit électronique[938]. Il s'impose, selon lui, d'être attentif « aux différentes fonctions généralement assignées à l'exigence de production d'un écrit »[939]. Tantôt, l'écrit n'est qu'une formalité de preuve ; tantôt, l'existence d'un écrit conditionne la validité de l'acte. L'importance de cette réflexion est d'ailleurs confirmée

[937] *M.B.,* 1er juillet 2004.

[938] D. De Roy, « L'accès aux documents administratifs dans un environnement dématérialisé », *in L'accès aux documents administratifs* (dir. D. Renders), *op. cit.,* pp. 837-839.

[939] *Ibid.,* p. 838.

par l'adoption de normes organisant la dématérialisation des procédures administratives, comme en matière de marchés publics par exemple. Il s'agit, pour le législateur, de déterminer les conditions de l'assimilation d'un écrit traditionnel à un écrit électronique, ce qui prouve qu'une telle assimilation ne peut être faite trop hâtivement.

b) L'optimisme. Bien que la prudence soit de mise, on trouve dans les réflexions de Cécile de Terwangne une source d'optimisme pour le citoyen désireux d'exercer son droit d'accès par la voie électronique. Même dans le silence de la loi, deux impératifs doivent encourager l'administration à accepter les demandes électroniques.

D'une part, *la loi du changement,* rappelée par la Charte de l'utilisateur des services publics[940], incite l'administration à s'adapter aux évolutions techniques[941]. Ainsi, « toutes les prestations fournies au titre de mission d'intérêt général dans le domaine de l'information publique doivent être progressivement et continuellement adaptées pour demeurer satisfaisantes au vu de l'évolution de la société »[942]. L'administration est donc encouragée à utiliser les moyens nouveaux à sa disposition, parmi lesquels figurent le courriel et le fax.

D'autre part, *la règle d'équivalence interne-externe* conduit à la même conclusion[943]. Cette règle consiste à soutenir que « l'administration doit rendre l'information accessible au public dans son état de conditionnement élaboré pour les besoins internes »[944]. Appliquée à la question présente, cette règle signifie que si, pour répondre à ses besoins propres, l'administration recourt aux échanges électroniques de courrier, il doit en être de même avec le citoyen.

§2. La formulation de la demande

258.- La matière et/ou le document recherché. Comme le prévoit l'article 5 de la loi du 11 avril 1994, la demande d'accès doit indiquer

---

[940] Voy. *supra* n° 239.-

[941] Précisions néanmoins qu'à ce jour, il ne semble pas qu'on puisse déduire de la loi du changement une réelle obligation, pour l'administration, de s'adapter aux évolutions techniques. À ce sujet, voy. *infra,* n° 381.-

[942] C. DE TERWANGNE, *Société de l'information et mission publique d'information*, *op. cit.*, p. 323.

[943] La règle d'équivalence interne-externe est également appelée « principe de réciprocité des avantages ». Ce principe est développée dans la suite de la recherche (voy. *infra* n°s 382.-et s.)

[944] *Ibid.*, pp. 297-298.

« clairement la matière concernée, et, si possible, les documents administratifs concernés ».

En d'autres termes, puisqu'il peut se contenter de mentionner la matière dont il veut prendre connaissance, le citoyen n'est pas contraint d'identifier précisément les documents auxquels il désire accéder. Cette solution est justifiée par le fait qu'« eu égard à la complexité de l'administration, on peut en effet supposer que ce ne sera que dans des cas exceptionnels que le demandeur pourra préciser les documents dont il aura besoin »[945].

Bien qu'on puisse affirmer que, ce faisant, « le législateur a placé le seuil très bas en ce qui concerne le contenu de la demande »[946], on se demande dans quelle mesure l'article 5 de la loi du 11 avril 1994 est suffisamment adapté à l'e-gouvernement. Dans ce contexte, la formulation d'une demande de document est difficile. À qui l'adresser ? L'usage des technologies génère-t-il des documents et, dans l'affirmative, comment savoir ce qui existe ? Ces questions sont importantes car si la demande n'est pas formulée correctement, elle pourra être rejetée.

1. La difficulté de formuler une demande dans le contexte de l'e-gouvernement

259.- De l'administration en silos à l'administration en réseaux. Comme cela a été évoqué dans le titre premier, l'usage des technologies provoque une modification substantielle dans la structure et le fonctionnement de l'administration. Progressivement, on passe d'une administration en silos à une administration en réseaux. Confronter l'exercice du droit d'accès dans l'administration en silos et dans l'administration en réseaux éclaire les particularités du droit d'accès dans le contexte actuel.

260.- Le droit d'accès dans l'administration en silos. Le droit d'accès aux documents administratifs a été pensé dans les années nonante, par rapport à la structure et aux moyens d'action de l'administration traditionnelle, alors organisée en silos.

a) Quant à la structure. À l'époque, des ministères étaient créés par rapport aux besoins d'intérêt général à satisfaire : la justice, les finances,

[945] Projet de loi relatif à la publicité de l'administration, Amendement n° 58, *Doc. Parl.*, Ch. Repr., sess. 1992-1993, n° 1112/4, p. 3.

[946] F. SCHRAM, La publicité de l'administration, Première partie : Commentaire – 2. La législation fédérale, Bruxelles, Politeia, 2010, p. 38.

l'agriculture, les affaires étrangères, la défense nationale, etc.[947]. Chaque ministère constituait « une administration autonome »[948], un « tout fonctionnellement et organiquement structuré »[949]. À la tête du ministère se trouvait un ministre administrant « seul son département sans en référer aux collègues »[950]. Dans ce contexte, le citoyen souhaitant prendre connaissance d'un document relatif à un domaine particulier de l'administration devait identifier le ministère compétent en cette matière et s'adresser à lui. En outre, son dossier personnel dans ce domaine était détenu, dans son intégralité, auprès dudit ministère. L'administré avait donc une seule institution comme interlocuteur, qu'il pouvait identifier par rapport aux compétences de cette dernière.

b) Quant aux moyens d'action. Outre la structure administrative fondée sur les matières à gérer, les moyens d'action de l'administration étaient également assez prévisibles pour les citoyens. En effet, pour accomplir ses missions, l'administration avait à sa disposition des agents humains dont le travail reposait sur l'élaboration de raisonnements humains, en recourant éventuellement à des études analytiques, des tableaux, des formules de calcul, etc. Les documents administratifs, en version papier, étaient également assez classiques et consistaient principalement en des PV de réunions, des résultats d'enquête, des formulaires remplis par les personnes concernées, des décisions rendues par l'autorité. Autant de paramètres que le citoyen pouvait prévoir, imaginer, comprendre.

261.- Le droit d'accès dans l'administration en réseaux. Aujourd'hui, de plus en plus de services publics sont regroupés au sein d'un réseau sectoriel comprenant, en son cœur, une institution publique jouant le rôle de plateforme d'échanges d'informations. Ces réseaux sectoriels sont définis par rapport aux citoyens, envisagés comme des clients confrontés à des problèmes administratifs dans leur vie quotidienne.

Le premier titre a montré qu'une telle structure est profitable pour la compréhension de la structure administrative. En ce qui concerne plus particulièrement l'accès aux documents administratifs, on peut raisonnablement considérer que le citoyen est en mesure d'identifier aisément le réseau au sein duquel se trouve le document recherché.

---

[947] R. Wilkin, *L'administration publique belge,* Bruxelles, Bruylant, 1958, pp. 33-34 ; M. Vauthier, *Droit administratif,* Bruxelles, Larcier, 1950, p. 77 ; C. Cambier, *Droit administratif,* Bruxelles, Larcier, 1968, p. 26 ; J. Rivero, *Le droit administratif,* Paris, Dalloz, 1965, p. 305.

[948] R. Wilkin, *op. cit.,* p. 34.

[949] C. Cambier, *op. cit.*, p. 26.

[950] R. Wilkin, *op. cit.,* p. 34.

Par exemple, pour accéder à un document relatif à sa santé, le citoyen-client se tournera vers le réseau santé. Désireux de connaître comment est calculée sa pension, il se tournera vers le réseau Travail, etc.

Néanmoins, même s'il parvient à identifier le réseau au sein duquel se trouve le document, le citoyen risque d'éprouver des difficultés relatives la structure nouvelle mise en place et aux moyens d'action nouveaux utilisés.

a) Quant à la structure nouvelle. Des difficultés peuvent surgir pour identifier l'administration précise qui s'occupe d'une matière particulière ou qui détient le document recherché ainsi que pour reconstituer l'entièreté du dossier personnel d'un citoyen.

En ce qui concerne l'identification de l'administration compétente pour répondre à la demande d'accès, le détenteur du document n'est plus nécessairement une administration traditionnelle avec laquelle le citoyen est en contact pour la gestion de sa vie administrative. Il peut aussi s'agir d'une plateforme d'échange d'informations.

Par exemple, la table des données disponibles au sein du réseau de la sécurité sociale est détenue par la plateforme d'échanges qu'est la Banque-Carrefour de la sécurité sociale.

Par ailleurs, le citoyen qui souhaite accéder à l'entièreté de son dossier personnel dans un domaine particulier doit suivre un parcours complexe, lié au principe de la collecte unique des données et à l'utilisation corollaire des sources authentiques. Concrètement, à l'ère de l'e-gouvernement, le dossier personnel de chaque individu est éclaté entre plusieurs administrations, à savoir, celles qui détiennent une source authentique de données. Le citoyen curieux n'exerce donc plus son droit d'accès par rapport à une administration prise isolément. Il est confronté à un système dans lequel interviennent toutes les administrations responsables d'une source authentique contenant des données à son sujet.

Dès lors, pour savoir ce que l'administration sait de lui, le citoyen doit contacter une première administration. Celle-ci lui dira qu'elle n'est pas à même de lui fournir une copie de son dossier en entier. Bien souvent, elle ajoutera qu'elle ne dispose pas de la liste des administrations ayant les autres parties de son dossier puisqu'elle a dû passer par une plateforme d'échange pour se voir communiquer les informations sans savoir d'où elles provenaient. Le citoyen devra donc contacter la plateforme d'échanges pour obtenir une copie de son répertoire des références. Et, pour reconstituer son dossier complet, il devra contacter chaque institution y mentionnée.

b) Quant aux moyens d'action nouveaux. L'usage des technologies dans l'administration génère également la création de documents et d'outils d'un genre nouveau. Les agents humains existent toujours au sein des administrations. Mais leurs raisonnements sont soutenus, et parfois même remplacés, par des calculs informatiques puissants. Les études analytiques, les tableaux de comparaison, les formules de calcul, ont été engloutis par les ordinateurs. Ces automates gèrent, grâce à quelques clics depuis la souris des agents ou parfois même sans leur intervention, l'envoi des informations, leur mise à jour, leur classement, leur utilisation dans les décisions administratives.

Par conséquent, aux documents administratifs traditionnels se sont ajoutés des documents directement liés au fonctionnement de ces outils nouveaux. On pense, par exemple, aux répertoires de références, aux sources authentiques, aux logiciels permettant de détecter les fraudes à partir d'un amas de données, aux entrepôts de données, aux tables informatiques répertoriant les transferts d'informations, aux listes de « log » avec le nom de l'agent, l'heure et la date de la consultation effectuée, etc. Il y a fort à parier que, pour l'heure, le citoyen n'imagine pas, ou seulement de manière très floue, l'existence de ce type de documents et de ces outils nouveaux. En outre, même s'il parvient à y accéder, on peut se demander dans quelle mesure il pourra réellement en comprendre le contenu. Dès lors, dans l'ignorance partielle ou totale de ces nouveautés complexes, quelle est l'utilité d'un droit d'accès aux documents administratifs ?

262.- La transparence ébranlée par l'administration en réseaux. Compte tenu des difficultés rencontrées pour prendre connaissance des documents détenus par les administrations, la transparence de l'administration est mise à mal. Des solutions pourraient être élaborées par la voie de la publicité active, de manière à ce que le citoyen ait au moins connaissance des documents existants et de l'autorité qui les détient. Nous analysons cette voie dans les développements relatifs à la publicité active de l'administration[951].

2. Les exceptions à la publicité liées à la formulation de la demande

263.- Deux exceptions. En vertu de l'article 6, §3, 3° et 4° de la loi du 11 avril 1994, une demande d'accès « formulée de façon manifestement trop vague » ou « manifestement abusive » peut être rejetée par

[951] Voy. *infra* n^{os}302.- et s.

l'administration. Le citoyen confronté à l'e-gouvernement risque de se voir opposer de telles exceptions.

264.- L'indication d'une matière et le risque que la demande soit « formulée de façon manifestement trop vague »[952]**.** On l'a dit, le *citoyen* risque d'éprouver des difficultés à identifier certains documents en particulier compte tenu de la structure nouvelle de l'administration et des outils nouveaux mis à la disposition des autorités publiques. Il peut, certes, se contenter d'indiquer la « matière concernée ». Mais que signifient ces termes ? Lors des discussions préparatoires de la loi, l'obligation légale d'indiquer « clairement la matière concernée », a été jugée trop imprécise. Depuis lors, la question persiste.

> Comme l'a affirmé un parlementaire dans le cadre d'une proposition d'amendement, la possibilité de ne mentionner que « la matière concernée » « enlève toute signification au terme 'clairement'. Qu'est-ce que la matière concernée ? »[953].

L'administration semble, elle-aussi, déroutée lorsqu'il s'agit de documents générés par la mise en place de l'e-gouvernement. Ainsi, des demandes d'accès peuvent être considérées comme vagues car les agents de l'administration n'ont pas une vision claire des documents qui existent ni de leur emplacement dans les fichiers.

> En guise d'illustration, nous avons exercé notre droit d'accès auprès d'une administration qui fait partie du réseau de la sécurité sociale. Au vu de nos recherches, nous pensons que cette administration détient très probablement une ou plusieurs sources authentiques de données utilisée(s) par la Banque-Carrefour de la sécurité sociale. Néanmoins, n'ayant pas la référence d'un document précis indiquant le nom de cette source authentique et dressant la liste des données qu'elle contient, nous n'avons pu mentionner un ou plusieurs document(s) déterminé(s) dans notre demande. Nous avons donc demandé la copie des documents nous permettant de savoir « le nom des sources authentiques détenues dans cette administration et le type de données reprises ». Il nous a été répondu que la demande était trop vague mais que nous pouvions préciser notre demande en livrant une définition de la notion de « source authentique » ainsi qu'une description plus précise du « contexte ». Après avoir pris contact par téléphone avec cette administration, il est apparu que la Banque-Carrefour prenait effectivement des données dans leurs bases de données afin de les faire circuler dans le réseau de la sécurité sociale. Cependant, ces collectes et transferts de données

[952] Art. 6, §3, 4°, de la loi du 11 avril 1994.

[953] Projet de loi relative à la publicité de l'administration, Amendements, *Doc. Parl.*, Ch. Repr., sess. 1992-1993, n° 1112/2, p. 18.

> étant effectués de manière informatique, les agents de l'administration ne semblent pas avoir une vision très claire de ces traitements ni même des données qu'ils détiennent sous forme authentique dont ils sont pourtant censés garantir la fiabilité.

La question de la familiarité des agents de l'administration avec la matière est pourtant importante au regard du droit d'accès exercé par le citoyen. En pratique en effet, on apprécie le caractère manifestement trop vague d'une demande en se posant la question de savoir si « un fonctionnaire qui est familiarisé avec la matière sur laquelle portent les documents administratifs » peut « identifier les documents administratifs demandés »[954]. Comment faire, alors, si les agents de l'administration ne sont pas familiers avec cette matière ?

Il revient donc aux fonctionnaires d'acquérir une bonne connaissance de cette matière nouvelle. Ils y sont d'ailleurs invités en vertu de la loi du changement[955]. Compte tenu de l'obscurité des lois en la matière[956], du manque de doctrine et de jurisprudence tout comme de la rareté des formations juridiques existant dans ce domaine, ce n'est pas chose aisée. Mais, malgré ces écueils, on constate généralement que les agents de l'administration font preuve de beaucoup de bonne volonté pour appréhender la complexité de l'e-gouvernement, comme en témoigne l'exemple qui suit.

> L'ONEm s'interroge actuellement sur les types de données qui peuvent être communiqués à d'autres administrations ainsi que sur les types de données qu'il est autorisé à recevoir. Ces autorisations sont octroyées par un comité sectoriel[957]. L'ONEm a demandé à la Banque-Carrefour de la sécurité sociale d'obtenir la liste de ces types de données. C'est une démarche logique quand on sait que la Banque-Carrefour de la sécurité sociale détient une « table des autorisations » reprenant, pour chaque type de données, les autorisations octroyées. Malheureusement, la Banque-Carrefour de la sécurité sociale a répondu qu'elle n'était pas en mesure de fournir le document demandé. Dès lors, les agents de l'ONEm œuvrent pour le moment à la mise en place, à des fins internes, d'une base de données « in/out » reprenant les décisions d'autorisation relatives aux données que l'ONEm peut transmettre et recevoir[958].

---

[954] Commission d'accès aux documents administratifs, avis n° 2011/301, du 8 août 2011. Voy. égal. F. Schram, *La publicité de l'administration, Première partie : Commentaire – 2. La législation fédérale, op. cit.,* p. 38.

[955] Voy. *infra* n° 381.-

[956] Voy. le Titre I.

[957] Voy. *infra* n°s 534.- et s.

[958] Entretien avec un agent de l'ONEm le 27 juillet 2011.

À n'en pas douter, ce type d'initiatives devrait aider les fonctionnaires à répondre au mieux aux demandes d'accès des citoyens relatives à la structure et au fonctionnement de l'e-gouvernement.

De telles demandes sont, pour l'heure, assez rares. Bien souvent, elles sont réduites aux seules démarches d'une doctorante namuroise. Mais elles devraient se multiplier progressivement, grâce à une connaissance plus généralisée de cette matière.

265.- « La demande est manifestement abusive »[959]**.** L'administration qui considère qu'une demande est manifestement abusive peut la rejeter, en vertu de l'article 6, §3, 3° de la loi du 11 avril 1994.

a) Deux hypothèses. Concrètement, cette exception peut être invoquée dans deux hypothèses. La première hypothèse est celle du *dol* : la demande d'accès du citoyen est telle qu'elle manifeste une volonté de nuire[960].

> Il peut s'agir, par exemple, d'une volonté de gêner le bon fonctionnement de l'administration. Un citoyen risque de se voir opposer cette exception s'il formule, de manière répétée, des demandes d'accès portant sur des documents qui lui ont déjà été envoyés[961].

La deuxième hypothèse est celle de l'*effet perturbateur de la demande*. Même si elle ne manifeste pas une intention dolosive, la demande peut être manifestement abusive si elle perturbe le fonctionnement de l'administration en exigeant un tel effort aux agents que la continuité et la fluidité de leurs tâches de base en seraient ébranlées[962].

> Par exemple, peuvent entrer dans cette hypothèse, les demandes portant sur « d'innombrables documents qui nécessitent des recherches considérables et peuvent avoir pour effet de perturber le service »[963].

---

[959] Art. 6, §3, 3°, de la loi du 11 avril 1994.

[960] F. Schram, « Toegang tot milieu-nformatie op federaal niveau », *R.W.,* 2006-2007, p. 1115 ; D. Déom, T. Bombois et L. Gallez, « Les exceptions au droit d'accès aux documents administratifs », *L'accès aux documents administratifs, op. cit.,* p. 404.

[961] M. Deprez, « La transparence de l'administration fiscale », *in Transparence et droit à l'information,* Liège, Formation permanente CUP, 2002, p. 195.

[962] D. Déom, T. Bombois et L. Gallez, « Les exceptions au droit d'accès aux documents administratifs », *op. cit.,* p. 404 ; F. Schram, *La publicité de l'administration, Première partie : Commentaire – 2. La législation fédérale, op. cit.,* p. 48(4).

[963] Commission d'accès aux documents administratifs, avis n° 96/85, du 16 juillet 1996, *in Rapport annuel 1996,* Bruxelles, p. 59, cité par C. de Terwangne, *Société de l'information et mission publique d'information, op. cit.,* p. 341.

Vu la difficulté que semblent éprouver actuellement certains fonctionnaires face à l'e-gouvernement, on peut craindre une augmentation des demandes d'accès jugées manifestement abusives au motif qu'elles génèrent une perturbation dans le service.

b) La démonstration de l'effet perturbateur de la demande. Il est important de préciser que l'effet perturbateur d'une demande ne peut être invoqué à la légère. Il doit être démontré. Concrètement, cela signifie plusieurs choses.

Tout d'abord, l'administration ne pourrait considérer qu'une demande est manifestement abusive au motif que l'information à livrer est *complexe et suppose certains efforts* de la part des agents[964].

> Par exemple, si un citoyen demande à l'ONEm d'où proviennent les données qu'il utilise sans les avoir directement collectées lui-même, il faudra que ses agents effectuent des recherches, via la Banque-Carrefour de la sécurité sociale et/ou d'autres administrations, pour connaître l'origine des données, sans pouvoir prétendre qu'il s'agit là d'un exercice trop pesant.

En outre, l'administration ne pourrait pas rejeter une demande d'accès au seul motif que les documents demandés sont trop nombreux. Il faut que la recherche et la communication aient un effet perturbateur sur le bon déroulement du service. Or, l'usage des technologies facilite le travail de l'administration à ce niveau. Les documents sont répertoriés dans une base de données, et non plus dispersés dans plusieurs classeurs. On peut les retrouver en quelques clics grâce à des outils de recherches fonctionnant par mots-clés, sans devoir passer en revue de multiples dossiers. L'imprimante demande moins d'efforts qu'une photocopieuse. Certains envois peuvent se faire par courrier électronique, sans timbre, ni papier, ni trajet à la Poste, etc. On peut ainsi affirmer que « dans le monde informatisé, transmettre la totalité d'une base de données peut mobiliser nettement moins de temps et d'efforts que de retrouver une seule feuille de papier classée par un prédécesseur »[965].

Une administration ne pourrait pas non plus rejeter une demande d'accès au seul motif qu'il existe une *voie alternative* pour prendre connaissance des documents recherchés[966]. Cette précision est particulièrement importante à l'heure actuelle où de plus en plus d'administrations ont

---

[964] D. Déom, T. Bombois et L. Gallez, « Les exceptions au droit d'accès aux documents administratifs », *op. cit.,* p. 405.

[965] C. de Terwangne, *Société de l'information et mission publique d'information*, *op. cit.*, p. 341.

[966] D. Déom, T. Bombois et L. Gallez, « Les exceptions au droit d'accès aux documents administratifs », *op. cit.,* p. 405.

tendance à renvoyer la personne vers un site internet. Une telle attitude porte atteinte au droit d'accès des personnes ne disposant pas des moyens électroniques appropriés. Cette précision demeure pertinente même si l'utilisation des technologies et la lutte contre la 'fracture numérique' s'intensifient. En effet, la lecture de certains documents nécessite l'utilisation d'un logiciel coûteux. Un citoyen pourrait donc ne pas y accéder même s'il possède un ordinateur muni des logiciels traditionnels, un accès à l'internet ainsi qu'une adresse de courrier électronique[967].

> Il est par exemple inadmissible que la BCSS réponde à la demande d'accès portant sur la copie de la table des données disponibles au sein du réseau de la sécurité sociale en renvoyant le citoyen à son site internet. Cela revient à refuser l'octroi d'une copie du document recherché. En outre, vu la complexité du site internet auquel le citoyen est renvoyé, la réponse de la BCSS consiste à exiger du demandeur qu'il reconstitue lui-même le document[968]

Enfin, le caractère manifestement abusif d'une demande « ne peut être invoqué si les gros efforts que nécessite une demande pour l'administration sont dus à une *mauvaise organisation* de l'administration elle-même »[969]. Même si les règles sont floues, et dès lors, difficilement compréhensibles, et même si les documents générés présentent parfois un aspect nouveau voire étrange, il revient à l'administration de s'adapter à ces évolutions afin d'être en mesure de fournir une réponse adéquate aux demandes d'accès. Les difficultés que génère le développement de l'e-gouvernement au sein des services administratifs ne peuvent peser sur les citoyens.

§3. L'objet de la demande

266.- Un document administratif. Que la demande soit formulée à partir d'une matière déterminée ou d'un document en particulier, elle a pour objet un ou plusieurs documents au(x)quel(s) le citoyen souhaite accéder. L'article 32 de la Constitution consacre le droit d'accès à l'égard de « tout document administratif ». L'article 1, b), 2°, de la loi du 11 avril 1994 définit cette notion comme « toute information, sous quelque forme que ce soit, dont une autorité administrative dispose ».

---

967 D. De Roy, « L'accès aux documents administratifs dans un environnement dématérialisé », *op. cit.,* p. 840.

968 Voy. *infra,* n° 299.-

969 F. Schram, *La publicité de l'administration, Première partie : Commentaire – 2. La législation fédérale*, *op. cit.*, p. 48 (4).

Cette notion est particulièrement large, tant en ce qui concerne sa forme que son contenu.

1. La forme du document

267.- Des supports multiples. Les travaux préparatoires de l'article 32 de la Constitution contiennent une longue énumération, non exhaustive, des documents soumis au droit d'accès. On peut en déduire que toute information, quel qu'en soit le support, est soumise à la transparence, du moment qu'une autorité administrative en dispose[970]. En outre, la notion de « document administratif » est beaucoup plus large que celle d' « acte administratif ». Ainsi, les actes préparatoires aux décisions administratives répondent également à la qualité de document administratif[971].

> Les travaux préparatoires de l'article 32 de la Constitution soulignent que « le terme 'document administratif' [...] doit être pris au sens large. Il concerne toutes les informations disponibles, quel que soit le support : documents écrits, enregistrements sonores et visuels y compris les données reprises dans le traitement automatisé de l'information. Les rapports, les études, même de commissions consultatives non officielles, certains comptes-rendus et procès-verbaux, les statistiques, les directives administratives, les circulaires, les contrats et licences, les registres d'enquête publique, les cahiers d'examen, les films, les photos, etc., dont dispose une autorité son en règle générale publics »[972].

268.- Le document administratif électronique. Étant donné que la loi du 11 avril 1994 soumet à la transparence toute information « sous quelque forme que ce soit », on doit considérer que la notion de document est *« a technically and technologically independant concept »*[973]. Les documents administratifs électroniques sont donc également visés par le droit d'accès. En d'autres termes, un citoyen peut demander d'accéder aux logiciels et aux fichiers informatiques.

Cette affirmation a bénéficié d'une reconnaissance jurisprudentielle au travers d'un arrêt du Conseil d'État en 2001. La haute juridiction

---

970 Sur l'autorité adminstrative, voy. *infra,* n°s 288.- et s.

971 Rapport fait au nom de la commission de la révision de la Constitution et des réformes des institutions, *Doc. Parl.,* Sénat, sess. 1992-1993, n° 100-49/2°, p. 8.

972 Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, *Doc. Parl.,* Ch. repr., session 1992-1993, n° 839/1, p. 5. Cette énumération est reprise dans les travaux préparatoires de la loi du 11 avril 1994.

973 F. SCHRAM, « Access to Administrative Documents in Belgium : an Example of Transparency within the European Unio », *R.E.D.C.,* 2011, pp. 663-699.

administrative soutient ainsi que le « document administratif [est une] notion englobant les logiciels de vote automatisé »[974], ce qui comprend les codes sources et les mesures de sécurité.

> Dans l'affaire qui a donné lieu à l'arrêt précité, le requérant demandait l'accès aux documents relatifs au vote automatisé, en ce compris le contenu des programmes informatiques utilisés. À cette occasion, le Conseil d'État a affirmé l'importance de pouvoir accéder à un tel outil informatique, soutenant que tout citoyen doit avoir « la possibilité [...] de s'assurer lui-même de la fiabilité des systèmes de vote et de dépouillement automatisés »[975], et ce, même si des experts informaticiens sont déjà désignés pour accomplir cette tâche.

Dans le même sens, plus récemment, la CADA a considéré que si les informations demandées se trouvent « par exemple dans un dossier électronique avec le logiciel disponible, la Commission ne voit aucune raison de refuser l'accès à ces informations »[976].

On peut raisonnablement considérer que ces interprétations peuvent être étendues à l'ensemble des documents électroniques.

269.- Le document potentiel. Lorsque les travaux préparatoires de l'article 32 de la Constitution et de la loi du 11 avril 1994 précisent que l'information est accessible « quel que soit le support », cela suppose qu'elle se trouve sur un support, c'est-à-dire qu'elle soit matérialisée[977].

Dans le contexte de l'e-gouvernement, il y a lieu de se demander si le critère de la matérialisation de l'information en un document particulier ne devrait pas être actualisé. En effet, dans l'administration papier, les informations étaient fixées sur un support physique, palpable : du papier, une disquette, une cassette vidéo, un cd-rom, etc. Dans l'e-gouvernement, il existe des informations qui se trouvent dans des bases de données. Elles ne sont pas fixées sur un support matériel mais elles pourraient l'être aisément grâce aux logiciels et aux ordinateurs mis à disposition de l'administration. Il s'agit là de « documents potentiels »[978]. Dans quelle mesure

---

[974] C.E., arrêt *Antoun,* n° 95.677, du 21 mai 2001. Au sujet de cet arrêt, voy. D. De Roy, « L'accès aux documents administratifs dans un environnement dématérialisé », *op. cit.,* p. 831.

[975] C.E., arrêt *Antoun, op. cit.*, p. 10.

[976] Commission d'accès aux documents administratifs, avis n° 2011-298, du 8 août 2011, p. 3.

[977] F. Schram, *La publicité de l'administration, Première partie : Commentaire – 2. La législation fédérale*, *op. cit.*, p. 20.

[978] C. de Terwangne, *Société de l'information et mission publique d'information*, *op. cit.*, pp. 325 et s.

peut-on obliger l'administration à effectuer cette extraction d'informations à partir des bases de données dont elle dispose ? C'est une question à laquelle on tente de répondre dans la suite de la recherche[979].

2. Le contenu du document

270.- Considérations générales. Des règles particulières sont liées au contenu du document. Elles visent les documents à caractère personnel et les documents inachevés ou incomplets.

a) Le document revêt un caractère personnel

271.- La preuve d'un intérêt. Au moment d'introduire la demande d'accès, il s'impose de savoir si le document auquel l'accès est demandé est un document à caractère personnel. En effet, de la réponse à cette question dépend la nécessité d'établir, ou non, l'existence d'un intérêt dans le chef du demandeur d'accès.

En principe, l'accès à un document administratif ne suppose pas la preuve d'un intérêt[980]. Comme l'a précisé le Conseil d'État, « tout administré a un intérêt actuel à exercer ce droit, quel que soit l'usage qu'il compte faire ultérieurement des documents dont il a pris connaissance »[981]. Le citoyen peut exercer ce droit quelles que soient les raisons qui le motivent car « l'exercice d'un droit fondamental ne saurait, en règle, être illégitime »[982].

Par contre, si l'accès concerne un document à caractère personnel, le demandeur doit justifier d'un intérêt, comme l'impose l'article 4, alinéa 2, de la loi du 11 avril 1994.

272.- La notion de document à caractère personnel. La loi du 11 avril 1994 définit le document à caractère personnel comme un « document administratif comportant une appréciation ou un jugement de valeur relatif à une personne physique nommément désignée ou aisément identifiable, ou la description d'un comportement dont la divulgation peut manifestement causer un préjudice à cette personne »[983]. Comme l'a encore récemment précisé la CADA, « il n'est donc pas suffisant qu'un

979 *Voy. infra* n°s 293.- et s.
980 Projet de loi relatif à la publicité de l'administration, Exposé des motifs, *op. cit.*, p. 13.
981 C.E., arrêt *Jacques Matagne,* n° 66.860, du 18 juin 1997, pp. 4 et 5.
982 *Ibid.,* p. 5.
983 Art. 1, 3°, de la loi du 11 avril 1994.

document administratif porte sur une personne physique pour pouvoir être considéré comme un document à caractère personnel »[984].

> Par exemple, ont été considérés comme des documents à caractère personnel, un rapport hiérarchique d'un chef de service concernant un fonctionnaire[985], le dossier constitué dans le cadre d'une procédure d'engagement[986], l'évaluation du président d'une administration parastatale dans le cadre d'une procédure en révocation en raison de sa conduite[987]. Certaines pièces du dossier fiscal d'un contribuable peuvent également être considérées comme un document à caractère personnel[988].

273.- La notion d'intérêt. L'intérêt requis pour accéder à un document à caractère personnel doit s'entendre de l'intérêt exigé pour la recevabilité d'une requête en annulation portée devant le Conseil d'État[989].

Le Conseil d'État et la CADA considèrent que l'intérêt est toujours présent dans le chef du demandeur qui souhaite accéder à ses propres documents à caractère personnel, c'est-à-dire, aux informations qui n'ont trait qu'à lui-même[990]. Il peut accéder à ses documents à caractère personnel quelle que soit la raison qui le motive, et même si les documents visés n'ont pas d'influence néfaste sur sa situation administrative ou juridique[991]. En effet, on estime que le citoyen doit être en mesure de vérifier tous les documents qui le concernent afin de pouvoir rectifier les éventuelles erreurs qui les affecteraient[992].

> Par exemple, la CADA a jugé que « vu que Monsieur X. était lui-même candidat à la promotion au poste de directeur régional de l'administration fiscale de Namur, il fait preuve dans tous les cas de l'intérêt requis pour accéder aux documents à caractère personnel le concernant »[993].

---

984 CADA, avis du 4 avril 2011, n° 2011-164.

985 C.E., arrêt *Duez,* n° 70.844, du 16 janvier 1998.

986 CADA, avis du 30 août 2002, n° 2002-66.

987 CADA, avis du 11 mai 2009, n° 2009-34.

988 C.E., arrêt *Louis,* n° 94.082, du 16 mars 2001.

989 Projet de loi relatif à la publicité de l'administration, Exposé des motifs, *op. cit.*, p. 14. Voy. l'article 19 des lois coordonnées sur le Conseil d'État, du 12 janvier 1973.

990 Voy., not., C.E., arrêt *Bvba S.L.A. Trading Company,* n° 156.628, du 20 mars 2006 ; Commission d'accès aux documents administratifs, avis n° 2009-25, du 20 avril 2009, p. 3.

991 F. Schram, *La publicité de l'administration, Première partie : Commentaire – 2. La législation fédérale*, *op. cit.*, p. 28.

992 Commission d'accès aux documents administratifs, avis n° 2000-37 du 8 mai 2000.

993 Commission d'accès aux documents administratifs, avis n° 2009-04, du 9 mars 2009, p. 3.

> C'est la raison pour laquelle un contribuable peut accéder à son dossier fiscal sans justifier d'un intérêt[994].

Par contre, une personne qui souhaite accéder à des documents personnels ayant trait à des tiers doit établir l'existence d'un intérêt certain et direct, légitime, actuel et suffisamment individualisé[995].

> Par exemple, la CADA a estimé que le candidat à une procédure de sélection présente l'intérêt requis pour accéder notamment aux « notes des membres du jury et procès-verbaux relatifs à l'ensemble des épreuves qui ont été présentées par les candidats »[996].

274.- Document à caractère personnel et document contenant une ou des donnée(s) à caractère personnel. Comme en témoigne cette recherche, l'étude de l'e-gouvernement en appelle fréquemment à l'usage des termes « document contenant une ou des données à caractère personnel ». Cette notion se distingue de la notion de « document à caractère personnel ».

Quand elles sont confrontées à des demandes d'accès relatives à de tels documents, les administrations sont soumises tant au respect de la loi du 8 décembre 1992 – qui protège les données à caractère personnel enregistrées dans des fichiers – qu'au respect de la loi du 11 avril 1994. Pour autant, les notions de « document à caractère personnel » et de « document contenant des données à caractère personnel » ne peuvent être confondues.

Une donnée à caractère personnel est, comme on l'a dit, toute information concernant une personne physique identifiée ou identifiable[997].

> Par exemple, un document reprenant le numéro de plaque d'immatriculation d'un administré est donc un document contenant une donnée à caractère personnel. L'utilisation qui en est faite est soumise au respect de la loi du 8 décembre 1992.

Un « document à caractère personnel » est une notion plus étroite que celle de « document contenant une ou des données à caractère personnel ». Ces deux notions ont en commun de concerner une personne identifiée ou identifiable. Mais, à la différence du document contenant une ou des données à caractère personnel, le document à caractère personnel

---

994 C.E., arrêt *Louis*, précité.

995 P. LEWALLE, *Contentieux administratif*, 3e éd., Bruxelles, Larcier, 2008, pp. 783-798.

996 Commission d'accès aux documents administratifs, avis n° 2011-07, du 14 février 2011.

997 Art. 1, 1°, de la loi du 8 décembre 1992.

contient une appréciation ou un jugement de valeur sur la personne concernée ou la description d'un comportement qui, s'il est divulgué, pourrait manifestement nuire à cette dernière.

En d'autres termes, tous les documents à caractère personnel sont des documents contenant une ou des données à caractère personnel, à condition qu'ils soient détenus sous une forme électronique ou sous une forme structurée[998], ce qui, aujourd'hui, est le plus souvent le cas. Mais un document contenant une ou des données à caractère personnel n'est pas nécessairement un document à caractère personnel.

> Par exemple, la CPVP reconnaît que peut être soumis à la loi du 8 décembre 1992 le dossier de nomination d'un inspecteur des finances, contenant des notes du Ministre des Finances et du Collège des chefs de service, relatives à l'état psychologique de cet inspecteur[999]. La loi du 8 décembre 1992 est applicable à ce dossier dans la mesure où « le dossier de nomination formerait une partie intégrante du dossier administratif, qui présenterait un niveau de structuration suffisant ou qui serait traité, en tout ou en partie, à l'aide de procédés automatisés ». Par ailleurs, ce dossier contient la description du comportement de la personne concernée dont la divulgation peut manifestement lui causer préjudice. Il s'agit donc également d'un document à caractère personnel soumis au respect de la loi du 11 avril 1994.

b) Le document est inachevé ou incomplet

275.- Les documents éclairant l'e-gouvernement. L'e-gouvernement est, à maints égards, très complexe. Il est, la plupart du temps, inconnu des juristes qui maîtrisent peu le droit des nouvelles technologies, tant cette matière est neuve et les questions soulevées, inédites.

Pourtant, nombre de personnes sont appelées à se prononcer sur la constitutionnalité et la légalité des nouveaux outils techniques utilisés dans l'administration et des traitements de données à caractère personnel

[998] Il peut s'agir d'une base de données informatique ou d'un fichier papier si les documents sont classés suivant une structure logique devant permettre une consultation aisée.

[999] La note du Ministre précise que « même si le candidat avait obtenu la mention 'très bien', il n'avait aucune chance d'être nommé à la fonction d'inspecteur. L'aptitude et les mérites font également partie des critères qui entrent en considération » (CPVP, avis n° 06/97 du 19 février 1997 relatif à l'utilisation de données concernant les jours de maladie et évaluation de données relatives à la santé dans le cadre d'une procédure de promotion au sein du Ministère des Finances, p. 2). Une autre note reprend une évaluation de l'état psychique de cet inspecteur, réalisée par une personne n'ayant pas la qualité de praticien de l'art de guérir et qui soutient que cet agent « zou te kampen hebben met ernstige psychische problemen, waardoor hij zich niet in staat zou achten zijn functie van hoofdcontroleur op een degelijke manier waar te nemen » (CPVP, avis n° 06/97 précité, p. 2)

qu'ils génèrent. On pense notamment aux personnes qui œuvrent au sein de la CPVP qui rend des avis sur ces problématiques nouvelles. On pense également aux membres des comités sectoriels, chargés d'autoriser, ou non, les traitements de données mis en place[1000]. Ces organes d'avis et de décision doivent se prononcer en connaissance de cause. On peut donc raisonnablement penser que chaque problématique qui leur est soumise s'accompagne de la remise de documents expliquant l'outil nouveau ou le traitement de données soumis à leur appréciation. En d'autres termes, ces institutions détiennent maints documents susceptibles d'offrir des informations éclairantes au sujet de l'e-gouvernement.

> Par exemple, en discutant avec un informaticien collaborant au fonctionnement de l'entrepôt de données OASIS, nous avons appris qu'un document d'environ 150 pages, décrivant le fonctionnement de cet outil de traitement de données, a été soumis au Comité sectoriel de la sécurité sociale dans le cadre des autorisations de traitements demandées.

276.- L'article 6, §3, 1°, de la loi du 11 avril 1994. L'accès à ces études relatives à l'e-gouvernement pourrait être refusé en vertu de l'article 6, §3, 1°, de la loi du 11 avril 1994 qui prévoit que « l'autorité administrative fédérale peut rejeter une demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif dans la mesure où la demande concerne un document administratif dont la divulgation peut être source de méprise, le document étant inachevé ou incomplet ».

En d'autres termes, un document peut être maintenu confidentiel s'il est source de méprise en raison de son caractère inachevé ou incomplet.

> Nous en avons fait l'expérience. Par lettre du 2 juillet 2011, nous avons demandé au Comité sectoriel de la sécurité sociale et de la santé de pouvoir accéder au document décrivant le fonctionnement d'OASIS. Par lettre du 11 août 2011, le Comité sectoriel de la sécurité sociale et de la santé nous a informée que cet accès nous était refusé au motif que, notamment, « de manière générale, il apparaît que les dossiers de demande soumis au Comité sectoriel de la sécurité sociale et de la santé en vue d'obtenir l'autorisation d'un communication de données sociales à caractère personnel sont par nature source de méprise dans la mesure où ils ne lient pas le Comité et ne présagent pas de sa décision d'autorisation ou des modalités de celle-ci et ne peuvent par conséquent jamais être considérés comme définitifs. En particulier et en outre, il ressort en l'espèce de l'analyse des dossiers soumis en 2000 et en 2005 au Comité sectoriel en vue des délibérations n° 01/06 du 6 mars 2001 et n° 05/01 du 18 janvier 2005, que les documents qui les

[1000] Voy. Titre III.

> constituent sont des documents principalement techniques, qui datent de nombreuses années et risquent, vu leur âge, d'être totalement dépassés et de ne pas (plus) répondre à vos questions avec la pertinence souhaitée ».

Au vu de la réponse donnée en l'espèce par le Comité sectoriel de la sécurité sociale et de la santé et compte tenu du fait qu'on peut craindre qu'une telle réaction soit également adoptée à l'égard d'autres documents détenus par d'autres institutions, il s'impose de revenir sur les deux conditions cumulatives qui composent l'exception étudiée à savoir, le fait que le document doit être inachevé ou incomplet, d'une part, et que sa divulgation doit être source de méprise, d'autre part.

277.- Un document inachevé ou incomplet.

a) Un document inachevé. Un document inachevé est un document à l'état de simple projet[1001]. Cette notion n'est pas nécessairement assimilable à celle de document préparatoire. La précision est importante car « les autorités ont démontré une certaine tendance à invoquer cette exception à mauvais escient »[1002], refusant ainsi d'offrir l'accès à des documents préparatoires à une décision, alors que ceux-ci sont en principe publics. En d'autres termes, un document peut être achevé alors qu'il a été élaboré au moment où la décision à laquelle il a servi n'était pas encore adoptée. Inversement, un document peut être inachevé alors que la décision à laquelle il a servi a déjà été prise[1003].

> Il a ainsi été soutenu lors des travaux préparatoires de la loi du 11 avril 1994 que « définir un 'document administratif' comme étant un document sur lequel il a déjà été statué est trop restrictif. Il y a lieu de considérer également comme document administratif les documents qui revêtent une importance dans le cadre de la prise de décision ou qui y ont contribué »[1004].

b) Un document incomplet. Un document incomplet est achevé, mais lacunaire[1005]. Le caractère lacunaire du document peut être lié au fait que

---

[1001] Commission d'accès aux documents administratifs, avis n° 94/33 et 95/12 cités par C. DE TERWANGNE, « Le droit à la transparence administrative », *op. cit.,* p. 17.

[1002] C. DE TERWANGNE, *op. cit.,* p. 26. Dans le même sens, R. ANDERSEN, « La mise en balance des intérêts en cause dans l'appréciation des motifs d'exception à la publicité de l'administration », *op. cit.,* p. 45.

[1003] D. DÉOM, T. BOMBOIS et L. GALLEZ, *op. cit.,* pp. 406 et 407 ; A. GOSSERIES, « Droit d'accès à l'information, documents inachevés et risque de méprise », *op. cit.*, p. 240.

[1004] Projet de loi relatif à la publicité de l'administration, Rapport fait au nom de la commission de l'intérieur, des affaires générales et de la fonction publique par L. Peeters, *op. cit*, p. 33.

[1005] D. DÉOM, T. BOMBOIS et L. GALLEZ, *op. cit.,* p. 406.

des informations ont dû être supprimées car leur divulgation aurait porté atteinte à l'un des intérêts protégés par l'article 6, §1, de la loi du 11 avril 1994 et dont il sera question ci-après[1006].

278.- Un document source de méprise. L'exception au droit d'accès prévue par l'article 6, §3, 1° de la loi du 11 avril 1994 s'applique aux documents inachevés ou incomplets *et* qui sont source de méprise, c'est-à-dire, qui risquent d'être mal interprétés par le demandeur d'accès. Leur communication générerait des malentendus.

Cette exception ne s'applique donc pas aux documents achevés et complets, même s'ils sont source de méprise (par exemple, en raison de leur complexité), ni aux documents inachevés ou incomplets, qui ne sont pas source de méprise. Précisons qu'il y a lieu d'être attentif au fait qu'un document source de méprise ne peut, comme tel, être écarté du droit à la transparence. Il faut que le risque de méprise soit lié à son caractère inachevé ou incomplet, ce qui doit être démontré par l'administration qui fait valoir cette exception[1007].

On peut s'étonner de cette exception. En effet, l'administration est tenue de donner des explications relatives au document divulgué[1008]. Si les explications adéquates sont données, comment considérer qu'il y a encore risque de méprise ?

En ce sens, la Commission d'accès aux documents administratifs a soutenu que l'existence de l'exception relative au risque de méprise ne devait pas empêcher l'administration de fournir des renseignements complémentaires pour empêcher la réalisation de ce risque[1009].

Dans cette ligne, Axel Gosseries pose la question de savoir s'il ne faudrait pas comprendre l'exception « risque de méprise », comme « constitutive d'une obligation de clarification en cas de risque de méprise plutôt que d'un motif d'exception »[1010]. Le « risque de méprise » devrait consti-

---

[1006] *Ibid.*

[1007] *Ibid.* ; A. Gosseries, « Droit d'accès à l'information, documents inachevés et risque de méprise », *op. cit.*, p. 241 et références citées ; C. de Terwangne, « Le droit à la transparence administrative », *op. cit.,* p. 26 qui cite un arrêt du Conseil d'État (arrêt *Luc Sevenhans,* n° 202.459, du 29 mars 2010). Dans cette affaire, il s'agissait d'une demande d'accès à une étude concernant l'hôpital militaire de Neder-Over-Hembeek. L'autorité militaire refusait d'octroyer l'accès à ce document au motif que cela affecterait la sérénité qui devait régner dans ce dossier. Le Conseil d'État a annulé la décision de l'autorité militaire.

[1008] Voy. *infra*, n° 300.-

[1009] CADA, avis 94/43 du 19 décembre 1994 cité par A. Gosseries, « Droit d'accès à l'information, documents inachevés et risque de méprise », *op. cit.*, p. 241.

[1010] A. Gosseries, « Droit d'accès à l'information, documents inachevés et risque de méprise », *op. cit.*, p. 241.

tuer, non une excuse pour ne pas divulguer le document, mais un motif de fournir des explications complémentaires.

3. Les exceptions à la publicité liées au contenu du document

279.- Deux catégories d'exceptions. La loi du 11 avril 1994 prévoit, en son article 6, §§ 1 et 2, des exceptions relatives au contenu du document auquel l'accès est demandé. Parmi les motifs d'exceptions que le législateur fédéral a « énumérés en vrac »[1011], on peut identifier une première catégorie d'exceptions visant à protéger le *bon fonctionnement des services publics*. Elle couvre la sécurité de la population, les relations internationales fédérales de la Belgique, l'ordre public, l'intérêt économique et financier de l'État, la recherche et la poursuite des faits punissables.

Une deuxième catégorie d'exceptions peut être circonscrite, qui repose sur la *protection d'intérêt de tiers*. La vie privée, le secret professionnel, le secret des affaires en font partie[1012].

280.- L'obligation de motivation. Chaque exception invoquée doit être pleinement motivée. En effet, une décision de refus d'accès est un acte administratif qui doit répondre au prescrit de la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs. Par conséquent, l'autorité administrative qui décide de maintenir un document confidentiel est tenue d'expliquer précisément pourquoi un motif d'exception est applicable à l'espèce[1013]. Cette motivation doit se faire *in concreto,* et non de manière abstraite[1014]. Il ne peut être question d'invoquer ces exceptions sans nuance.

[1011] R. Andersen, « La mise en balance des intérêts en cause dans l'appréciation des motifs d'exception à la publicité de l'administration », *op. cit.,* p. 41.

[1012] Des exceptions techniques, fonctionnelles ressortissent à une troisième catégorie. Il s'agit notamment des exceptions relatives à la formulation de la demande et au caractère inachevé ou incomplet d'un document, dont il a été question précédemment (D. Déom, T. Bombois et L. Gallez, « Les exceptions au droit d'accès aux documents administratifs », *L'accès aux documents administratifs, op. cit.,* p. 214).

[1013] A. Mast, J. Dujardin, M. Van Damme et J. Vande Lanotte, *Overzicht van het Belgisch Administratief Recht,* Mechelen, Kluwer, 2009, p. 751 ; P. Lewalle, *Contentieux administratif, op. cit.,* p. 83.

[1014] A. Mast, J. Dujardin, M. Van Damme et J. Vande Lanotte, *op. cit.*, p. 75 et références jurisprudentielles citées. Pour un cas d'application concernant l'exception relative à la vie privée, voy. Commission d'accès aux documents administratifs, avis n° 2009-29 du 20 avril 2009 : « un motif d'exception ne peut cependant être invoqué que lorsqu'il ressort d'éléments concrets du document administratif demandé qu'une publicité portera atteinte à la vie privée de tiers [...] Une autorité administrative ne peut se limiter à des formules d'ordre général pour refuser une publicité ».

Cette obligation de motivation, applicable à toutes les exceptions prévues par la loi, conduit à relativiser la distinction faite parmi les exceptions reprises à l'article 6 de la loi du 11 avril 1994. On a coutume de distinguer les exceptions obligatoires et absolues – elles sont reprises à l'article 6, §2 – de celles qui sont obligatoires et relatives, figurant à l'article 6, §1. Dans le premier cas de figure, l'autorité administrative doit refuser l'accès au document dont la publicité porterait atteinte à l'un des impératifs énumérés, sans effectuer de mise en balance des intérêts en jeu[1015]. Dans le deuxième cas de figure, la demande d'accès ne peut être refusée que s'il est établi, au regard des intérêts mentionnés dans l'article 6, §1, de la loi, que la confidentialité du document doit primer sur sa divulgation[1016].

Concrètement, si l'exception invoquée est *relative*, l'autorité sollicitée doit justifier en quoi la publicité du document porte atteinte à l'un des intérêts repris à l'article 6, §1, de la loi, et en quoi cet intérêt prime sur l'intérêt de la publicité.

Si l'exception invoquée est *absolue*, l'examen que l'administration doit effectuer n'est pas fort différent du précédent, contrairement à ce que l'on serait tenté de croire à la lecture de la loi. En effet, une exception absolue ne peut être invoquée de manière automatique. L'autorité administrative doit, tout d'abord, établir concrètement que la divulgation du document porterait atteinte à l'un des intérêts protégés. Cela suppose l'exercice d'un large pouvoir d'appréciation de la part de l'administration, étant donné que lesdits intérêts sont formulés de manière vague. Ensuite, quand bien même l'atteinte serait établie, l'exception pourrait céder devant d'autres impératifs[1017], de sorte qu'on doit admettre que « même l'exception dite absolue donne donc lieu à une certaine balance, sinon des intérêts, du moins des droits en présence »[1018].

Quoi qu'il en soit, certaines exceptions en particulier peuvent faire obstacle au droit d'accès du citoyen confronté à l'e-gouvernement.

[1015] L'art. 6, §2, de la loi du 11 avril 1994 utilise une formule impérative en disposant que « l'autorité [...] rejette la demande [...] si la publication du document administratif porte atteinte à [...] ».

[1016] L'art. 6, §1, de la loi du 11 avril 1994 prévoit que « l'autorité [...] rejette la demande [...] si elle a constaté que l'intérêt de la publicité n l'emporte pas sur la protection de l'un de intérêts suivants [...] ».

[1017] Diane Déom, Thomas Bombois et Laurence Gallez évoquent la jurisprudence en matière fiscale, qui admet que la confidentialité d'un dossier fiscal au nom de la protection de la vie privée du contribuable, doit être actée au profit du droit d'un autre contribuable – un exe-conjoint, par exemple – de connaître les éléments à partir desquels est calculée la dette fiscale (D. Déom, T. Bombois et L. Gallez, *op. cit.,* pp. 217 et 218).

[1018] D. Déom, T. Bombois et L. Gallez, *op. cit.,* p. 218.

a) Les exceptions invoquées dans le contexte de l'e-gouvernement

i. Les exceptions protégeant le bon fonctionnement du service public

281.- E-gouvernement et bon fonctionnement du service public. Les exceptions protégeant le bon fonctionnement du service public présentent un intérêt particulier dans le contexte de l'e-gouvernement. En effet, comme on l'a déjà dit à plusieurs reprises, une justification régulièrement avancée pour soutenir l'usage des technologies est la volonté d'augmenter l'efficacité de l'administration. Il en va d'autant plus ainsi qu'à cette fin, l'informatique offre de belles promesses.

En particulier, la protection des intérêts financiers de l'État au travers d'une amélioration de la lutte contre la fraude fiscale et sociale reçoit une attention soutenue dans les développements de l'e-gouvernement. Des outils ont été créés dans cette optique. Ils se fondent notamment sur la définition de profils de fraudeurs et l'identification d'indices de fraude. Un citoyen peut-il accéder aux documents qui contiennent de telles informations ? Deux cas concrets illustrent l'intérêt de cette interrogation.

> Un dentiste est régulièrement contrôlé par l'INAMI. Il demande à accéder à son dossier individuel, détenu par la Commission de Profils de l'INAMI, afin de comprendre la raison pour laquelle il fait l'objet de ces contrôles. La Commission de Profils est hésitante. En effet, dans ce dossier, se trouve notamment un document reprenant des profils statistiques qui permettent de comparer l'activité de ce dentiste par rapport à l'activité moyenne de tous les praticiens de l'art dentaire. En outre, la lecture de ce document permet de connaître les critères utilisés par la Commission de Profils pour identifier les dentistes qui sont de potentiels fraudeurs, et le critère qui, en l'espèce, a convaincu l'INAMI de porter ses suspicions sur ce dentiste.
>
> L'accès au document d'environ 150 pages relatif au fonctionnement d'OASIS, dont il a été question plus haut, devrait permettre de comprendre comment fonctionne cet entrepôt de données, et quelles sont les données qui y sont reprises.

282.- Le droit du citoyen face au devoir de l'administration. La réponse à la question qui vient d'être soulevée est délicate. On perçoit d'emblée la tension créée entre le droit du citoyen et le devoir de l'administration.

D'une part, en vertu de l'article 32 de la Constitution et de la loi du 11 avril 1994, le citoyen a le droit de connaître tous les éléments sur lesquels se fonde une décision qui le concerne[1019]. Il doit notamment pou-

[1019] C.E., arrêt *Matagne, op. cit.,* p. 7.

voir vérifier l'exactitude des informations qui conduisent l'administration à contrôler ses actes. En outre, de manière générale, l'administré a le droit de prendre connaissance de tous les documents qui composent son environnement administratif, de manière à contrôler la qualité, l'objectivité et l'impartialité de l'action administrative.

D'autre part, l'administration doit pouvoir accomplir ses missions. Le contrôle de la fraude fiscale et sociale en fait partie. Aujourd'hui, ce contrôle est facilité par l'utilisation d'indices de fraude appliqués aux données personnelles des administrés. On peut aisément et rapidement extraire des bases de données le nom des individus qui répondent au profil d'un fraudeur, avec une forte présomption que cela s'avère exact une fois le contrôle concret effectué. De toute évidence, en communiquant aux citoyens les indices de fraude utilisés et les profils de fraudeur constitués, l'administration peut craindre que les personnes concernées réorientent leur comportement de manière à ne pas correspondre aux profils définis. Plus encore, elle peut redouter que de nouveaux schémas de fraude soient élaborés, en dehors des critères déjà connus de l'administration qui permettraient de repérer les fraudeurs potentiels. C'est la raison pour laquelle, dans les deux cas mentionnés ci-avant, l'accès aux documents en question a été refusé. Dans les deux cas, la décision de refus se fonde sur l'article 6, §1, de la loi du 11 avril 1994 : la publicité du document porterait atteinte, d'une part, à la recherche ou la poursuite de faits punissables (article 6, §1, 5° de ladite loi) et, d'autre part, à un intérêt économique ou financier fédéral (article 6, §1, 6°, de ladite loi).

> Un raisonnement semblable a été tenu par le Conseil d'État au sujet de la demande d'accès d'un contribuable à son dossier fiscal. La demande a, à juste titre selon le Conseil d'État, été refusée étant donné qu'on a considéré que la connaissance des documents visés permettrait à ce contribuable de savoir ce que l'administration fiscale connaissait à son sujet, de manière à lui éviter d'aller trop loin dans les aveux spontanés…[1020] Ce qui convainc du refus d'accès est « une évaluation du risque que ce comportement ou ce genre de comportement fait peser sur la capacité du fisc à opérer correctement sa tâche »[1021].
>
> Le Conseil d'État l'a rappelé dans un cas concernant la perception des impôts. La haute juridiction a soutenu que l'exception relative à la protection d'un intérêt économique ou financier de l'État peut être invoquée pour refuser l'accès à un document si l'État belge indique « concrètement les motifs pour lesquels il estime que l'intérêt de la publicité ne justifie pas une communication prématurée des informations [...] et si la mise en

[1020] C.E., arrêt *Jongen,* n° 137.660, du 25 novembre 2004.
[1021] D. Déom, T. Bombois et L. Gallez, *op. cit.,* p. 223.

balance des intérêts effectuée n'est pas déraisonnable, la motivation du refus d'accès étant par ailleurs conforme à l'observation de la commission d'accès aux documents administratifs »[1022].

Dans les deux cas exposés précédemment, il s'agit d'outils d'investigation, dans le but d'identifier les fraudeurs. La décision de refus n'est correctement motivée qu'à la condition d'expliquer en quoi la divulgation du document mettrait en cause le travail d'investigation des deux organes en question.

ii. Les exceptions protégeant l'intérêt de tiers

283.- E-gouvernement, protection de la vie privée et protection du secret professionnel. Parmi les exceptions protégeant l'intérêt des tiers, deux exceptions en particulier intéressent l'e-gouvernement. Il s'agit de la vie privée (article 6, §2, 1°) et du secret professionnel (article 6, §2, 2°).

284.- L'exception protégeant la vie privée. En vertu de l'article 6, §2, 1°, la vie privée est un motif d'exception qui revêt un caractère absolu. Cela signifie que l'autorité doit refuser l'accès au document dès qu'il est établi que la divulgation de celui-ci constitue une ingérence dans la vie privée de tiers[1023].

Si la demande d'accès concerne un document administratif contenant des données à caractère personnel, il y a lieu de combiner cette exception avec la loi du 8 décembre 1992 à laquelle l'administration est également soumise. Cela signifie que le document contenant des données à caractère personnel ne pourra pas être communiqué s'il porte atteinte à la loi du 8 décembre 1992[1024]. L'exception protégeant la vie privée, consacrée dans la loi du 11 avril 1994, pourra être avancée. En effet, la communication d'un document contenant des données à caractère personnel est un traitement de données, au sens de la loi du 8 décembre 1992. L'administra-

[1022] C.E., arrêt *Tassin,* n° 97.056, p. 12 et arrêt *S.C.R.L. « AS »,* n° 97.057, p. 12 du 27 juin 2001.

[1023] Cette exception absolue fait l'objet de critiques à maints égards, compte tenu du fait que le législateur semble ainsi faire primer systématiquement le droit fondamental à la vie privée sur le droit fondamental à la transparence administrative, ce qui paraît difficilement justifiable. Voy. D. Déom, T. Bombois et L. Gallez, « Les exceptions au droit d'accès aux documents administratifs », *op. cit.,* pp. 332-337 ; C. de Terwangne, « Le droit à la transparence administrative », *op. cit.,* pp. 24-25.

[1024] F. Schram, « Access to Administrative Documents in Belgium : an Example of Transparency within the European Union », *op. cit.,* p. 676. Cet auteur s'étonne d'ailleurs du fait qu'en pratique, on ne distingue pas suffisamment la protection des données à caractère personnel de la protection de la vie privée. Voy. à ce sujet, F. Schram, « Anderhalf jaar werking van de beroepinstantie Openbaarheid van bestuur », *C.D.P.K.*, 2006, pp. 564 à 567, spec. p. 565.

tion saisie de la demande doit donc être attentive à la proportionnalité de ce traitement. Pour ce faire, elle doit mettre en balance l'intérêt, pour le demandeur, d'obtenir la communication du document, et les risques qu'une telle communication entraînerait pour la personne visée dans ce document. Selon que l'intérêt de la communication prime, ou non, le document sera divulgué, ou non. La nature des données à caractère personnel contenues dans le document visé est particulièrement importante pour cet examen.

Ainsi, si les données sont des données sensibles, telles que des données relatives à l'état de santé, l'appartenance raciale ou religieuse, on aura tendance à considérer que le document ne peut être communiqué, à moins que l'intérêt de la communication soit vraiment supérieur à celui de la non-divulgation. Pour le dire autrement, l'autorité peut invoquer l'exception protégeant la vie privée si la communication porte atteinte à la vie privée au sens strict, c'est-à-dire la vie privée dans le sens « intimité ». Cette méthode d'interprétation respecte la règle selon laquelle les exceptions au droit d'accès sont d'interprétation stricte[1025]. Elle se rapproche d'ailleurs de la solution organisée par la loi du 11 avril 1994 pour la communication les documents à caractère personnel. Dans cette hypothèse, rappelons que la communication ne peut avoir lieu que si le demandeur d'accès prouve l'existence d'un « intérêt », étant donné que le document renferme un jugement de valeur et, dès lors, des données embarrassantes.

En revanche, si le document contient des données à caractère personnel dont la divulgation respecte la loi du 8 décembre 1992, la communication pourra avoir lieu. On pense, par exemple, au PV d'une réunion mentionnant seulement la présence de la personne à cette réunion, ou à un document contenant des données relatives à la carrière professionnelles[1026].

285.- L'exception protégeant le secret professionnel. Plusieurs lois relatives à l'e-gouvernement imposent une obligation de secret professionnel aux personnes qui effectuent des traitements de données ou sont amenées à en prendre connaissance dans l'exercice de leurs tâches professionnelles.

[1025] A. MAST, J. DUJARDIN, M. VAN DAMME et J. VANDE LANOTTE, *op. cit.*, p. 727.

[1026] La CADA a considéré que ne relevaient pas de la vie privée les données relatives à la carrière professionnelle (CADA, avis 95/51, cité par D. VOORHOOF, « Openbaarheid van bestuur in provincies en gemeenten. Het passief recht op openbaarheid. De uitzonderingensgronden en hun toepassing, met toelichting op basis van de advies van de CTB », *in Een open en behoorlijk bestuur. Openbaarheid en klachtenbehandeling bik locale besturen* (dir. M. SUYKENS), Brugge, Van den Broele, 1998, Deel a. III, p. 23).

Ainsi, plusieurs lois disposent que « les personnes qui, dans l'exercice de leurs fonctions, interviennent dans les missions d'enregistrement, de mémorisation, de gestion et de mise à disposition des données [traitées par l'outil concerné] ou qui ont connaissance de telles données, sont tenues au secret professionnel »[1027]. Cette disposition est formulée de manière si floue qu'elle pourrait être utilisée pour refuser l'accès à tout document qui est passé sous les yeux d'une personne impliquée dans un traitement de données et ce, même si le document demandé ne contient pas de données à caractère personnel.

La loi sur la Banque-Carrefour de la sécurité sociale impose, en outre, une obligation de secret professionnel au « Président du comité sectoriel de la sécurité sociale et de la santé ainsi que tous les autres membres du comité à tous les membres ou les experts associés » et ce, « pour tout ce dont ils ont pu avoir connaissance en raison de leurs fonctions »[1028]. C'est également un motif d'exception qui a été invoqué par le comité sectoriel de la sécurité sociale et de la santé pour nous refuser l'accès au document relatif au fonctionnement d'OASIS. Signalons que seuls les membres du Comité sectoriel de la sécurité sociale et de la santé bénéficient d'un secret professionnel aussi large.

À nouveau, cette exception ne peut pas être interprétée trop largement. On ne pourrait admettre que le secret professionnel soit invoqué en soi, de manière abstraite. Cette exception doit être justifiée en pratique, au regard de la raison d'être d'une telle obligation de confidentialité.

b) La conciliation du droit d'accès et des intérêts protégés

286.- La divulgation de la partie restante. La nécessité de maintenir une partie du document confidentielle ne justifie pas la confidentialité du document dans son ensemble. En effet, l'article 6, §4, de la loi du 11 avril 1994, dispose que « lorsque, en application des §§ 1er à 3, un document administratif ne doit ou ne peut être soustrait que partiellement à la publicité, la consultation, l'explication ou la communication sous forme de copie est limitée à la partie restante ».

En d'autres termes, il revient à l'administration de communiquer le document demandé après avoir omis de celui-ci les éléments dont la divulgation porterait atteinte à l'un des intérêts protégés. Le seul motif qui pourrait justifier la confidentialité de l'entièreté du document est à

[1027] Art. 27 de la loi du la Banque-Carrefour des véhicules ; art. 29 de la loi sur la Banque Carrefour des entreprises ; art. 11 de la loi organisant un registre national des personnes physiques ; art. 28 de la loi sur la Banque-Carrefour de la sécurité sociale.

[1028] Art. 47, al. 3, de la loi sur la Banque-Carrefour de la sécurité sociale.

trouver dans l'article 6, §3, 1°, de la loi du 11 avril 1994, à savoir, le fait que le caractère incomplet du document serait source de méprise[1029].

B. La réponse de l'autorité

287.- L'autorité soumise au droit d'accès. En vertu de l'article 4 de la loi du 11 avril 1994, le droit d'accès aux documents administratifs s'exerce à l'égard des institutions ayant la qualité d'autorité administrative fédérale[1030]. En outre, l'institution sollicitée doit disposer du document administratif recherché[1031].

§1. Une autorité administrative

288.- Considérations générales. La loi du 11 avril 1994 subordonne la transparence administrative à l'existence d'une autorité administrative. Cette notion suscite maintes critiques tant elle est floue et, dès lors, difficile à utiliser. Des solutions sont proposées dans les présents développements.

1. Les difficultés générées par la notion d'autorité administrative

289.- Une notion floue. La loi du 11 avril 1994 se réfère à la notion d'autorité administrative, qui doit être comprise au sens de l'article 14 des Lois coordonnées sur la Conseil d'État[1032]. Initialement, le législateur a été séduit par la référence à cette notion flexible et évolutive qui permettrait d'adapter progressivement le champ d'application de la législation aux évolutions de la matière[1033]. Pourtant, déjà durant les discussions préparatoires de la loi du 11 avril 1994, la complexité de cette notion a été mise en exergue. Certains parlementaires ont proposé un amendement

---

[1029] Voy. *supra,* n° 278.-

[1030] Les autres législations d'accès ne s'appliquent également qu'aux autorités administratives, hormis le décret flamand sur lequel nous revenons ci après. À ce sujet, voy. P. Lewalle, L. Donnay et G. Rosoux, *op. cit.,* pp. 35-37.

[1031] Cette affirmation se déduit de l'art. 1, b), 2° et de l'art. 5 de la loi du 11 avril 1994.

[1032] Art. 1, b°, 1° de la loi du 11 avril 1994.

[1033] R. Andersen, « Conclusions générales », *in L'accès aux documents administratifs* (dir. D. Renders), *op. cit.*, p. 960 ; M. Boes, « Openbaarheid van bestuur – Bevoegdheidverdeling – De federale openbaarheidswetgevings », *in Openbaarheid van bestuur in Vlaanderen, België en de Europese instellingen,* Leuven, Instituut vorr Milieurecht K.U. Leuven, 1996, p. 16.

remplaçant le renvoi aux Lois coordonnées sur le Conseil d'État par une définition plus précise de l'autorité administrative[1034].

> À propos de la notion d'autorité administrative, il a ainsi été soutenu, à juste titre selon nous, que « si l'on tient à renforcer la publicité de l'administration, il y a d'ores et déjà lieu de simplifier au maximum le texte de la loi. Il faut en effet, que le citoyen, qui retire le bénéfice essentiel de cette nouvelle législation, puisse comprendre au mieux ces dispositions dont il peut espérer tirer profit »[1035]. En outre, il a été souligné que « le législateur doit prendre ses responsabilités et ne pas laisser au Conseil d'État le soin de définir le champ d'application » de la loi[1036]. Le ministre a jugé la discussion « particulièrement intéressante » mais y a mis fin estimant « qu'il est difficile d'en voir les limites ». Et d'estimer l'adoption de l'amendement « quelque peu prématurée »[1037]. Il a encouragé la solution actuelle, soutenant que « quiconque est un tant soit peu familiarisé avec cette matière saura donc à quoi s'en tenir »[1038].

Aujourd'hui, les critiques persistent à l'égard de ces termes, notamment en raison du fait que la notion d'autorité administrative ne dépend pas seulement de la jurisprudence du Conseil d'État. La Cour constitutionnelle et la Cour de cassation en définissent également les contours, au gré d'une jurisprudence évolutive[1039]. En outre, les critiques sont d'autant plus acerbes que la notion d'autorité administrative conditionne ici l'exercice d'un droit fondamental, celui de la transparence administrative consacré à l'article 32 de la Constitution. Certains se demandent si l'utilisation d'un terme si

---

[1034] Ainsi était-il proposé de remplacer le renvoi à l'article 14 des lois coordonnées sur le Conseil d'État par la définition suivante « 1° autorité administrative : l'administration fédérale, l'organisme public et le service public assimilé ressortissant à une autorité administrative fédérale, ainsi que la personne privée, la personne morale ou l'association de fait chargée par une autorité fédérale de l'exercice d'un service public fédéral » (Projet de loi relatif à la publicité de l'administration, Rapport fait au nom de la commission de l'intérieur, des affaires générales et de la fonction publique par L. Peeters, *op. cit.*, pp. 13-14). Une discussion semblable a également eu lieu au Sénat. Voy. le Rapport fait au nom de la Commission de l'Intérieur par M. Pinoie, *Doc. Parl.,* Sénat, sess. 1993-1994, n° 999-2, pp. 13-15.

[1035] Projet de loi relatif à la publicité de l'administration, Rapport fait au nom de la commission de l'intérieur, des affaires générales et de la fonction publique par L. Peeters, *op. cit.*, p. 38.

[1036] Rapport fait au nom de la Commission de l'Intérieur par M. Pinoie, *op. cit.,* p. 13.

[1037] Projet de loi relatif à la publicité de l'administration, Rapport fait au nom de la commission de l'intérieur, des affaires générales et de la fonction publique par L. Peeters, *op. cit.*, p. 38.

[1038] Rapport fait au nom de la Commission de l'Intérieur par M. Pinoie, *op. cit.,* p. 14.

[1039] M. Leroy, *Contentieux administratif*, 3e éd., Bruxelles, Bruylant, 2004, p. 268 ; P. Lewalle, *Contentieux administratif*, *op. cit.,* p. 642 ; X. Delgrange et B. Lombaert, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : questions d'actualité », *op. cit.,* pp. 19-23.

vague est souhaitable, étant donné que la notion d'autorité administrative au sens de l'article 14 des lois coordonnées « a déjà fait l'objet d'évolutions substantielles, qui ne sont fort probablement pas les dernières »[1040].

Le malaise qui entoure l'utilisation de la notion d'autorité administrative se renforce encore davantage dans le contexte de l'e-gouvernement. En effet, comme on a déjà pu le souligner, de nouvelles institutions apparaissent. L'identification de leur statut ne s'impose pas avec la force de l'évidence.

La notion d'autorité administrative sera étudiée dans le troisième titre de la recherche[1041]. Néanmoins, on peut déjà indiquer que des questions entourent, par exemple, le statut des comités sectoriels. Ces organes de décision sont chargés d'autoriser ou de refuser les échanges de données entre les administrations. Ils disposent donc du pouvoir de prendre des décisions obligatoires à l'égard de tiers. Néanmoins, étant institués au sein de la CPVP, on peut se demander si leur rattachement au pouvoir exécutif est suffisant pour leur attribuer la qualité d'autorité administrative. Il est surprenant de constater qu'au sein même du comité sectoriel de la sécurité sociale, on ne semble pas connaître la réponse à la question du statut de cette autorité, alors qu'il s'agit du comité sectoriel le plus productif pour le moment, qui doit contrôler de très nombreuses administrations. Ainsi, lors de notre demande d'accès au document relatif à OASIS, le président de ce comité sectoriel nous a répondu qu' « il n'est pas certain que la loi du 11 avril 1994 s'applique au Comité sectoriel de la sécurité sociale et de la santé. En effet, cette loi s'applique, en vertu de son article 1er, aux autorités administratives fédérales [...]. La doctrine, dont vous faites partie, considère que [...] les comités sectoriels ne constituent pas des autorités administratives au sens de l'article 14 des Lois coordonnées sur le Conseil d'État[1042] »[1043].

290.- Une notion restrictive. En ne visant que les autorités administratives, la loi du 11 avril 1994 limite le cercle des débiteurs du droit d'accès. La limitation du droit d'accès des citoyens au travers de l'exigence

---

[1040] M. Verdussen et A. Noël, « Les droits fondamentaux et la réforme constitutionnelle de 1993 », *A.P.T.,* 1994, p. 134, note 58. Dans le même sens, D. Renders, B. Gors et C. Thiebaut, *op. cit.,* p. 579 ; J. Sambon, « L'accès à l'information en matière d'environnement comme droit fondamental », *in L'accès aux documents administratifs* (dir. D. Renders), *op. cit.,* p. 242 ; C. de Terwangne, « Le droit à la transparence administrative », *op. cit.,* p. 14.

[1041] Voy. *infra,* nos 518.- et s.

[1042] E. Degrave, « La Commission de la protection de la vie privée : un organisme invincible ? » *R.D.T.I.*, 2006, n° 25, pp. 237-238.

[1043] Lettre du président du Comité sectoriel de la sécurité sociale, Yves Roger, du 11 août 2011.

d'une autorité administrative semble pourtant contraire à la volonté du constituant. En effet, tout au long des discussions qui ont précédé l'adoption de l'article 32 de la Constitution, une interprétation large du droit fondamental à la transparence administrative a été prônée.

> On a ainsi soutenu que la disposition constitutionnelle est volontairement succincte car « une spécification plus détaillée [...] ne fait que rétrécir le texte au lieu de l'éclaircir. Le danger est trop grand que ce qui n'est pas repris soit interprété comme une restriction volontaire ou involontaire »[1044]. Et d'ajouter que « le principe général sera la publicité des documents administratifs. Les restrictions ne pourront être interprétées largement »[1045].
>
> Quant aux autorités soumises au respect du droit d'accès, elles n'ont pas fait l'objet de discussions détaillées et ont été évoquées ci et là en usant indifféremment des termes « administration », « autorité ou service », ou « autorité administrative ». À propos de ces derniers termes, il a été dit que « l'interprétation concrète de cette notion sera faite par la suite. Etant donné qu'en l'occurrence, il s'agit d'un droit fondamental, une interprétation aussi large que possible devra être utilisée »[1046]. En guise d'exemple, il a été affirmé, à une seule reprise, qu' « on peut notamment renvoyer à l'article 14 des lois sur le Conseil d'État et la jurisprudence du Conseil d'État à ce sujet »[1047].
>
> La CADA abonde dans le même sens. Récemment, à l'occasion du recours que nous avons formé contre la décision de refus du Comité sectoriel de la sécurité sociale et de la santé de nous donner accès au document relatif à OASIS, elle a encore affirmé que « le [constituant] visait [...] un domaine d'application personnel très vaste, mais a laissé au législateur le soin de l'interpréter. Vu le fait qu'il s'agit d'un droit fondamental, le législateur doit opter pour un contenu aussi vaste que possible. Par ailleurs, lorsque pour l'interprétation du champ d'application personnel le législateur opte pour la notion 'd'autorité administrative', il ne peut pas interpréter cette notion de manière si restrictive que la loi serait en contradiction avec le champ d'application que le [constituant] envisageait »[1048]. S'agissant du Comité sectoriel de la sécurité sociale et de la santé, elle affirme que cette autorité « ne peut pas être considéré

[1044] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Note explicative, *op. cit.*, p. 4.

[1045] Révision du Titre II de la Constitution, en vue d'y insérer un article 24 *ter* relatif à la publicité et à la motivation des actes de l'administration, et au médiateur, Rapport fait au nom de la Commission de la révision de la Constitution et des réformes des institutions par M. Seeuws, *Doc. Parl.,* Sénat, sess. Extr. 1991-1992, n° 100-49/2°, p. 9.

[1046] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Note explicative, *op. cit.*, p. 5.

[1047] *Idem*.

[1048] Commission d'accès aux documents administratifs, avis n° 2011-309, du 10 octobre 2011, sur le refus de donner accès à des documents qui ont été utilisés par le Comité sectoriel de la sécurité sociale et de la santé pour prendre une décision.

> commune une autorité administrative telle que visée à l'article 14 des Lois coordonnées sur le Conseil d'État »[1049]. Néanmoins, elle prend soin d'ajouter que « bien que la Commission n'exclue pas que l'absence de toute protection juridique doive être considérée comme étant contraire aux articles 10 et 11 de la Constitution lorsque le Comité sectoriel de la Sécurité sociale et de la Santé prend une décision sur l'octroi d'autorisations, cela ne permet toutefois pas d'arriver à ce constat. Seule la Cour constitutionnelle peut faire un tel constat. La possibilité de s'adresser à la Cour constitutionnelle par le biais d'une demande préjudicielle est toutefois réservée aux juridictions »[1050].

Il y a donc lieu de s'interroger sur la constitutionnalité de la loi du 11 avril 1994[1051]. Comme l'affirme le professeur Sambon, « il n'y a en effet guère de sens à définir un régime de transparence administrative qui s'attache à tout document administratif – et non seulement aux actes administratifs – lorsque celui-ci s'applique aux seules autorités administratives disposant d'un pouvoir de décision unilatéral. Les instances consultatives, par les missions qui leur sont octroyées, sont à l'évidence des organismes à l'égard desquels un régime d'accès aux documents administratifs doit prioritairement être arrêté »[1052].

2. Des solutions envisageables

291.- L'application directe de l'article 32 de la Constitution. En l'état actuel des choses, un citoyen à qui l'on refuserait l'accès à un document administratif au motif que l'instance sollicitée n'est pas une autorité

[1049] *Ibid.,* p. 9.

[1050] *Ibid.,* pp. 9 et 10. Cette précision est importante. En effet, par cet avis juridique, les comités sectoriels sont à présent prévenus du fait que refuser l'accès aux documents administratifs qu'ils détiennent est très probablement inconstitutionnel, même si la Cour constitutionnelle n'a pas encore eu l'occasion de se prononcer à ce sujet. On peut dès lors se demander dans quelle mesure cet avis n'emporte pas l'obligation, pour les comités sectoriels, d'anticiper un futur constat d'inconstitutionnalité en ne refusant plus une demande d'accès au motif qu'ils ne sont pas des autorités administratives. Au sujet du droit, pour une administration, d'écarter l'application d'une disposition de valeur législative en raison de sa contrariété aux dispositions de droit interne dont la Cour constitutionnelle assure le respect, voy. R. Van Melsen, « Quelles personnes », *in L'article 159 de la Constitution. Le contrôle de légalité incident* (dir. M. nihoul), Bruxelles, La Charte, 2010, pp. 69 et s.

[1051] Dans le même sens, J. Sambon, « L'accès à l'information en matière d'environnement comme droit fondamental », *op. cit.,* p. 242 ; D. Renders, B. Gors et C. Thiebaut, *op. cit.,* p. 580 ; F. Schram, « Openbaarheid van bestuur en de burgelijke stand », *T.B.P.,* 1998, p. 396 ; C. de Terwangne, « Le droit à la transparence administrative », *op. cit.,* p. 15 ; J. Sambon, « L'accès à l'information en matière d'environnement comme droit fondamental », *op. cit.,* pp. 243 et 244.

[1052] J. Sambon, « L'accès à l'information en matière d'environnement comme droit fondamental », *op. cit.,* p. 242.

administrative n'est pas pour autant contraint de se résigner. En effet, l'article 32 de la Constitution est « *self executing* », comme cela a été affirmé à plusieurs reprises lors des discussions préalables à l'adoption de cette disposition. Concrètement, cela signifie que « même si les différents législateurs ne font pas usage de cette possibilité [de déterminer des exceptions et fixer les modalités de l'exercice du droit à la publicité], ce droit est néanmoins d'application »[1053].

On peut déduire de ces propos que les autorités qui, n'étant pas des autorités administratives, ne sont pas soumises à la loi du 11 avril 1994, sont néanmoins tenues de divulguer les documents en leur possession, en vertu de l'article 32 de la Constitution[1054].

292.- Une modification législative. Pour mettre fin à la situation anticonstitutionnelle que crée la loi du 11 avril 1994 en subordonnant la transparence administrative à la condition d'une autorité administrative, le législateur fédéral devrait élargir le spectre des instances soumises au droit d'accès. Pour ce faire, il pourrait s'inspirer de la solution adoptée dans le décret flamand relatif à la publicité administrative, et dans les législations d'accès à l'information en matière d'environnement.

a) L'article 3, 1°, du décret flamand du 26 mars 2004 relatif à la publicité de l'administration. Lors des discussions préparatoires au décret du 26 mars 2004 relatif à la publicité de l'administration, le législateur flamand n'a pas manqué de faire état de la « grande insécurité juridique » créée par la notion d'autorité administrative, d'ailleurs révélée par la jurisprudence du Conseil d'État et de la Cour de cassation[1055]. Les incertitudes créées ne semblaient pas conformes au prescrit

[1053] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Rapport fait au nom de la Commission de la révision de la Constitution, des Réformes institutionnelles et du règlement des conflits par M. Reynders, *op. cit.*, p. 8.

[1054] D. Renders, B. Gors et C. Thiebaut, *op. cit.,* p. 580 ; C. de Terwangne, « Le droit à la transparence administrative », *op. cit.,* pp. 4 et 5. Néanmoins, si une autorité refuse tout de même l'accès, la décision de refus ne pourra pas être attaquée devant le Conseil d'État mais bien devant le juge judiciaire puisque, dans cette hypothèse, l'autorité en question n'est pas une autorité administrative (D. Renders, B. Gors et C. Thiebaut, *op. cit.,* p. 580).

[1055] « Alhoewel het de bedoeling was van de decreetgever om door dit begrip zo te definiëren, een evolutief begrip in te voeren, heeft de recente evolutie in de rechtspraak van de Raad van State en van het Hof van Cassatie ertoe geleid dat grote rechtsonzekerheid ontstaan is omtrent het precieze toepassingsgebied » (Ontwerp van decreet betreffende de openbaarheid van bestuur, Memorie van toelichting, *Parl. St.*, Vlaams Parlement, sess. 2002-2003, n° 1732/1, p. 3.

de l'article 32 de la Constitution[1056] et ont eu des conséquences « inattendues et néfastes »[1057].

En 2004, il a donc été décidé d'abandonner la notion d'autorité administrative utilisée dans le décret flamand de 1999, et de la remplacer par la notion d' « instance administrative », qui a une portée beaucoup plus large[1058].

> Cette notion est définie à l'article 3, 1°, dudit décret :
>
> « On entend par 'instance administrative' :
>
> a) une personne morale créée par ou en vertu de la Constitution, d'une loi, d'un décret ou d'une ordonnance ;
>
> b) une personne physique, un groupement de personnes physiques, une personne morale ou un groupement de personnes morales dont le fonctionnement est déterminé et contrôlé par a) ;
>
> c) une personne physique, un groupement de personnes physiques, une personne morale ou un groupement de personnes morales, dans la mesure où ils sont chargés par une instance administrative dans le sens de a), de l'exécution d'une tâche d'intérêt général ou dans la mesure où ils défendent une tâche d'intérêt général et prennent des décisions liant des tiers ».

b) Les législations d'accès à l'information en matière d'environnement. Les législations d'accès à l'information en matière d'environnement transposent, au sein de la collectivité fédérale et des entités fédérées, la Convention d'Aarhus[1059] et la directive 2003/04/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès à l'information en matière d'environnement. Or, en vertu de ces normes, les obligations en matière de droit d'accès à l'environnement s'appliquent aux « autorités publiques », notion qui reçoit une définition large par ces textes. Dès lors, le cercle d'autorités visées par le droit d'accès à l'information environnementale dépasse largement celui constitué des seules autorités administratives[1060]. C'est pourquoi, les législations d'accès à l'information en matière d'environnement ne recourent pas à la notion

---

[1056] Ontwerp van decreet betreffende de openbaarheid van bestuur, Memorie van toelichting, *op. cit.,* p. 10.

[1057] *Ibid.*, p. 9.

[1058] F. Schram, "Access to Administrative Documents in Belgium : an Example of Transparency within the European Union", *op. cit.,* p. 685 ; du même auteur, "Anderhalf jaar werking van de beroepinstantie Openbaarheid van bestuur", *CDPK,* 2006, pp. 545-546 ; A. Mast, J. Dujardin, M. Van Damme et J. Vande Lanotte, *Overzicht van het Belgisch Administratief Recht*, *op.cit.,* pp. 737 et 738.

[1059] Convention sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement du 25 juin 1998.

[1060] Art. 2, §2, de la Convention d'Aarhus et art. 2, 2), de la directive 2003/04/CE précitée.

d'autorité administrative et soumettent davantage d'autorités aux obligations de transparence[1061].

> Par exemple, la loi du 5 août 2006 relative à l'accès du public à l'information en matière d'environnement[1062] utilise les termes « instance environnementale » pour traduire, en droit fédéral, la notion d'autorité publique développée dans la Convention d'Aarhus et la directive 2003/04/CE.
>
> L'article 3, 1°, de ladite loi définit l' « instance environnementale » de la sorte :
>
> a) une personne morale ou un organe créé par ou en vertu de la Constitution, d'une loi, d'un décret ou d'une règle visée à l'article 134 de la Constitution ;
>
> Le législateur vise, par là, « l'ensemble des institutions, ayant la personnalité juridique ou non, qui, *per se,* exercent des fonctions administratives »[1063].
>
> b) toute personne physique ou morale qui exerce des fonctions administratives publiques, y compris des tâches, activités ou services spécifiques en rapport avec l'environnement ;
>
> Ces termes couvrent « les personnes physiques ou morales qui, tout en ne relevant pas stricto sensu du secteur public, exercent, de par la loi ou un arrêté royal, des missions de service public »[1064].
>
> c) toute personne physique ou morale ayant des responsabilités ou des fonctions publiques, ou fournissant des services publics, en rapport avec l'environnement, sous le contrôle d'un organe ou d'une personne visé(e) au point a) ou b).
>
> Il s'agit de personnes privées dans la mesure où elles « exerceraient des fonctions publiques, par exemple dans le cadre d'une sous-traitance avec une administration ; en ce cas elles tomberaient dans le champ d'application de la loi pour la partie de leurs activités en rapport avec ces activités publiques »[1065].

Ainsi, les législations d'accès à l'information en matière d'environnement présentent la particularité intéressante de soumettre aux obligations de transparence l'ensemble des autorités publiques, qu'elles aient ou non un pouvoir de décision unilatéral, qu'elles soient, ou non, suffisamment rattachées au pouvoir exécutif. En outre, sont également soumises à ces législations d'accès, les entités qui détiennent des informations pour le compte des autorités publiques.

[1061] Pour de plus amples précisions, voy. J. SAMBON, « L'accès à l'information en matière d'environnement », *op. cit.,* pp. 676, 678 et 679.

[1062] *M.B.,* 28 août 2006.

[1063] Projet de loi relatif à l'accès du public à l'information en matière d'environnement, Exposé des motifs, *Doc. Parl.,* Ch. Repr., sess. 2005-2006, n° 51-2511/001, p. 12.

[1064] *Ibid.,* p. 13.

[1065] *Idem.*

Dans le contexte de l'e-gouvernement, un tel élargissement du champ d'application de la loi d'accès aux documents administratifs permettrait d'imposer, sans ambigüité, les obligations de transparence à des organismes comme la Banque-Carrefour de la sécurité sociale, les comités sectoriels, et même, les sous-traitants des administrations.

§2. Une autorité administrative qui dispose du document

293.- La détention matérielle du document et les questions soulevées. L'autorité administrative sollicitée par la demande d'accès doit disposer du document demandé pour pouvoir le communiquer. L'exigence de la détention matérielle du document pose plusieurs questions, particulièrement dans le contexte de l'e-gouvernement.

En effet, comme on l'a déjà souligné, le citoyen n'a pas une vision très claire des documents qui existent dans l'administration. Une autorité sollicitée, faisant preuve de mauvaise foi, pourrait dire qu'elle ne dispose pas du document. Comment apporter la preuve de cette détention ?

Par ailleurs, une autorité pourrait dire qu'elle ne dispose pas du document car celui-ci n'existe pas dans une forme matérielle, palpable. Mais il s'agit peut-être de documents potentiels que l'administration peut aisément transformer en documents matériels à l'aide des outils informatiques dont elle dispose. Dans quelle mesure peut-on l'astreindre à cette tâche ?

Finalement, l'e-gouvernement génère la création de documents parfois incompréhensibles. On pense à des tables informatiques. Le citoyen doit-il se résigner à recevoir la copie d'un document inintelligible ?

1. La preuve de la détention matérielle du document

294.- Le refus de mauvaise foi. Il peut arriver que l'autorité prétende ne pas disposer du document demandé et refuse de faire droit à la demande d'accès du citoyen.

> Nous en avons fait l'expérience. Nous avons demandé à la Banque-Carrefour la copie de la table des données disponibles au sein du réseau de la sécurité sociale. Rappelons qu'il s'agit d'une table « quoi-où » qui reprend le type de données disponibles auprès de quelle institution de sécurité sociale, ainsi que les conditions auxquelles ces données peuvent être communiquées. La Banque-Carrefour a refusé de nous en donner une copie, arguant du fait qu'elle « ne dispose pas d'un inventaire intégré de toutes les données disponibles auprès des différents acteurs du secteur social et ne peut donc pas vous le fournir en tant que tel »[1066].

[1066] Lettre de l'Administrateur général de la Banque-Carrefour de la sécurité sociale, Franck Robben, du 7 juillet 2010.

Une telle attitude laisse perplexe. La table « quoi-où » est une partie substantielle du répertoire des références, qui est à la base du fonctionnement de toute plateforme d'échange d'informations. En refusant de divulguer cette table, on ne peut s'empêcher de se demander s'il ne s'agit pas d'une manière, pour la Banque-Carrefour, de maintenir un certain pouvoir, issu de la détention de l'information[1067]. Le fait de laisser les administrations dans l'ombre, sans qu'elles sachent qui détient quoi et qui est susceptible de communiquer quoi, peut être perçu comme un moyen de se rendre incontournable.

295.- La preuve issue du caractère indispensable du document. L'autorité sollicitée ne peut pas prétendre qu'elle ne détient pas les documents recherchés si elle en est l'auteur ou que ces documents « lui sont indispensables pour exercer correctement sa mission et qu'ils lui ont normalement été transmis par l'autorité qui a délivré l'autorisation »[1068], comme l'affirme la CADA.

Ce motif peut être rétorqué à la Banque-Carrefour de la sécurité sociale. En effet, la table des données disponibles est non seulement un document établi par cette institution, mais également un document indispensable à son fonctionnement. En effet, elle ne pourrait collecter les données demandées dans la source authentique qui les détient et les acheminer vers l'autorité qui les réclame, sans savoir qui détient quoi, d'où le caractère indispensable de la table des données disponibles.

296.- La preuve issue de la publicité active. Même si la publicité active de l'administration demeure très sommaire[1069], il existe des portails internet faisant état de documents existants au sein des administrations. Ces documents existent donc et doivent être accessibles dans la mesure où leur divulgation ne se heurte à aucune exception légale.

Assez paradoxalement, la Banque-Carrefour de la sécurité sociale fait état de l'existence de la table des données disponibles, bien qu'elle refuse l'accès à ce document sous prétexte de ne pas en disposer. Ainsi, à plusieurs reprises, le site

[1067] Comme l'affirme un auteur, l'importance de l'enjeu de l'information administrative tient notamment au fait que l'administration « détient le savoir et donc le pouvoir d'un double point de vue : le savoir technique, c'est-à-dire la compétence d'une part, la maîtrise de l'information (non technique) à caractère politique (rapports de forces, alliances, négociations), d'autre part. En fait, l'information administration concerne ce double savoir » (C. Spanou, « Associations et information administrative », *in Information et transparence administratives, op. cit.,* p. 147).

[1068] Commission d'accès aux documents administratifs, avis 95/58 du 21 avril 1995, *Amén.- Env.,* 1995, p. 198. Voy. égal. C. de Terwangne, « Le droit à la transparence administrative », *op. cit.,* p. 19.

[1069] Voy. *infra,* n°s 302.- et s.

http://www.ksz.fgov.be/ indique l'existence de cette composante du répertoire des références et explique son contenu, sans pour autant le détailler.

2. Le document potentiel

297.- La notion de document potentiel. Un document potentiel peut être défini comme « un ensemble d'informations qui n'est pas fixé sur un support matériel mais qui peut potentiellement l'être par l'administration à l'aide des outils informatiques mis à sa disposition »[1070].

À l'étranger, différentes législations d'accès visent ce type de document.

La *Tryckfrihetsförordningen* suédoise[1071] prévoit, depuis 2002, qu'elle s'applique aux documents qui consistent en une « *compilation of informations taken from material recorded for automatic data processing* »[1072].

La *Laki viranomaistoiminnan julkisuudesta* finlandaise[1073] évoque les documents potentiels dans une section consacrée à la « *production of sets of data on request* ». Elle dispose que, moyennant le respect de certaines conditions, « *an authority may compile and deliver a set of data forms from signs contained in one or more computerised information management systems and maintained for various purposes* »[1074].

La loi sur l'accès à l'information canadienne affirme de manière très claire que « les documents qu'il est possible de préparer à partir d'un document informatisé relevant d'une institution fédérale sont eux-mêmes considérés comme relevant de celle-ci, même s'ils n'existent pas en tant que tels au moment où ils font l'objet d'une demande de communication »[1075].

298.- L'ampleur de la tâche imposée à l'administration. Les législations d'accès belges ne fixent aucun critère permettant de déterminer l'ampleur de la tâche que l'on peut exiger de l'administration lorsqu'il lui est demandé de créer un document administratif à partir d'un document potentiel.

[1070] Sur les caractéristiques d'un document potentiel, voy. C. DE TERWANGNE, *Société de l'information et mission publique d'information, op. cit.,* p. 325, n° 307 et les références citées.

[1071] Qui se traduit en anglais par *The Freedom of the Press Act*.

[1072] The Freedom of the Press Act, Chapitre 2, art. 3, al. 2.

[1073] Qui se traduit en anglais par *Act on the Openness of Government Activities* (621/1999). Voy. également The European Ombudsman, *Public access information in EU databases,* Strasbourg 2008, disponible sur le site http://www. ombudsman.europa.eu/resources/otherdocument.faces/en/4160/html.bookmark, p. 29.

[1074] Act on the Openness of Government Activities, Section 21 (1).

[1075] Loi sur l'accès à l'information, art. 4 (3), L.R. 1985, ch. A-1.

De toute évidence, une demande d'accès à un document potentiel ne peut aboutir à imposer à l'administration un travail d'une telle ampleur que la bonne exécution du service public en serait perturbée. Cela constituerait, en effet, une demande manifestement abusive, justifiant que la demande d'accès soit refusée[1076].

Ainsi, pour fixer les limites des efforts qui peuvent être imposés à l'administration lors d'une telle recherche d'informations, on peut se référer au critère des disponibilités techniques de l'administration et de la conformité de la demande avec les tâches administratives ordinaires[1077], à l'image des législations étrangères précédemment évoquées.

> La *Tryckfrihetsförordningen* suédoise se réfère au critère des « mesures de routine »[1078], c'est-à-dire, des mesures peu coûteuses qui ne requièrent pas des efforts extraordinaires[1079]. Cette notion est appréciée au cas par cas, ce qui permet la flexibilité nécessaire compte tenu de l'évolution rapide des outils technologiques[1080].
>
> La *Laki viranomaistoiminnan julkisuudesta* finlandaise indique qu'une telle demande d'accès doit être appréciée au regard du volume et de la qualité des données traitées[1081].
>
> L'*Electronic Freedom of Information Act* américain mentionne que les autorités doivent faire des « efforts raisonnables » pour rechercher les documents demandés, sauf « *when such efforts would significantly interfere with the operation of the agency's automated information system* »[1082].
>
> La loi sur l'accès à l'information canadienne n'impose un tel travail à l'institution sollicitée, que si celle-ci « a normalement à sa disposition le matériel, le logiciel et les compétences techniques nécessaires à la préparation »[1083].

299.- L'utilité de la notion dans l'e-gouvernement. L'intérêt, pour un citoyen, de pouvoir exiger de l'administration qu'elle crée un document administratif à partir d'un document potentiel se comprend assez

---

[1076] Voy. *supra,* n° 265.-

[1077] C. DE TERWANGNE, *Société de l'information et mission publique d'information*, *op. cit.*, p. 328, n° 309.

[1078] The Freedom of the Press Act, Chapitre 2, art. 3, al. 2.

[1079] P. SEIPEL, « Paper Laws in Transition », *in From Data protection to Knowledge Machines* (P. SEIPEL éd.), Computer Law series n° 5, Deventer, Boston, Kluwer Law and Taxation, 1990, p. 109 cité par C. DE TERWANGNE, *Société de l'information et mission publique d'information, op. cit.,* p. 328, n° 309.

[1080] The European Ombudsman, Public access information in EU databases, *op. cit.*, p. 30.

[1081] Act on the Openness of Government Activities, Section 21 (1).

[1082] Electronic Freedom of Information Act USC5, Section 552 (a) (3) (C).

[1083] Loi sur l'accès à l'information, art. 4 (3), L.R. 1985, ch. A-1.

bien au regard d'un double phénomène que connaît l'enregistrement de l'information aujourd'hui.

D'une part, le *support de l'information* détenue par l'administration a changé, comme on l'a souligné précédemment. Dans l'administration traditionnelle, l'information est disponible sur du papier. Seule l'information figurant sur le document peut être communiquée au citoyen. Dans l'e-gouvernement, l'information est enregistrée dans une base de données. On peut communiquer au citoyen la copie de la base de données. Mais on peut également extraire de cette base de données de nouvelles informations, en usant d'un logiciel qui permet de sélectionner certaines données, les comparer, etc.

D'autre part, la *localisation de l'information* connaît également des évolutions. Nombre d'administrations sont regroupées dans un réseau, au sein duquel elles collaborent en s'échangeant les informations. Des informations relatives à une même matière ou à un même document administratif sont donc disséminées, de manière décentralisée, entre les administrations du réseau. Elles sont stockées dans différentes bases de données. Le regroupement des informations relatives à la matière concernée par la demande ou encore la confection du document recherché suppose d'aller puiser les informations pertinentes en des fichiers distincts. C'est pourquoi, l'information administrative ne se réduit pas au contenu des documents existants. « Elle s'étend à toute donnée et à tout renseignement qui aident à situer le document précis dans son contexte, à apprécier sa valeur, et qui rendent [...] l'individu intéressé capable de l'utiliser »[1084].

Dans la mesure où l'extraction d'informations à partir d'une base de données, ou leur regroupement à partir de bases de données distinctes, n'impose pas un travail disproportionné à l'administration sollicitée, il lui revient de faire les manipulations informatiques nécessaires pour répondre à la demande d'accès du citoyen. Malheureusement, on constate que cet impératif n'est pas nécessairement respecté en pratique.

> Notre demande d'accès à la table des données disponibles, que détient la Banque-Carrefour de la sécurité sociale, illustre encore cette problématique.
>
> En effet, l'Administrateur général de cette institution nous a répondu d'une manière stupéfiante. Il avance que « la table des données disponibles est une table informatique contenant des références aux types de formulaires électroniques qui permettent d'obtenir des données auprès des différents acteurs du secteur social. Le site internet de la Banque-Carrefour de la sécurité sociale contient une description détaillée de tous ces formulaires

[1084] C. Spanou, « Associations et information administrative », *op. cit.*, p. 151.

électroniques en précisant les acteurs entre lesquels ils sont échangés en conformité avec les autorisations du Comité sectoriel de la sécurité sociale et de la santé ».

Et d'ajouter, « Pour en déduire[1085] les données disponibles auprès des différents acteurs du secteur social, il faut donc connaître le contenu de ces formulaires.

À cet effet, je vous invite à consulter notre site internet via les liens suivants :

http://www.ksz.fgov.be/fr/bcss/nodepage/content/websites/belgium/services/basic-services.html

http://www.ksz.fgov.be/fr/bcss/page/content/websites/belgium/services/service_citizen.html

http://www.ksz.fgov.be/fr/bcss/page/content/websites/belgium/services/service_employer.html

http://www.ksz.fgov.be/fr/bcss/nodepage/content/websites/belgium/services/service_institution.html »[1086]

En d'autres termes, la réponse de la Banque-Carrefour consiste à imposer au citoyen de retrouver lui-même les formulaires électroniques pertinents. De les parcourir. De les comprendre. Et d'extraire de chacun d'eux l'institution concernée et le type de données qu'elle détient. Après avoir dressé un schéma des institutions et des données détenues par celles-ci, le citoyen doit encore identifier quelles sont les données autorisées à sortir des sources authentiques, ainsi que les conditions qui entourent ces transferts.

Une telle attitude de la Banque-Carrefour est inadmissible. La solution offerte au citoyen est disproportionnée. On lui demande de réaliser un travail d'une ampleur extrême, qui probablement ne peut aboutir, alors que la tâche de la BCSS est bien plus aisée compte tenu des outils mis à sa disposition.

1. Une tâche aisée pour la Banque-Carrefour : un document potentiel. Il est évident que la Banque-Carrefour peut, en quelques clics, extraire de ses bases de données et, notamment, des formulaires électroniques et des autorisations du Comité sectoriel, un document reprenant les « chemins » informatiques qui ont été mis en place entre les institutions pour chaque type de données, et dès lors, le panorama des institutions et des données détenues par elles.

En effet, ces chemins informatiques existent : la Banque-Carrefour traite quotidiennement d'innombrables demandes de collectes indirectes de données sociales. Pour y répondre, il y a lieu de vérifier que la donnée est disponible dans le réseau et d'identifier la source authentique qui la détient.

[1085] C'est nous qui soulignons.

[1086] Lettre de l'Administrateur général de la Banque-Carrefour de la Sécurité sociale, Franck Robben, du 7 juin 2010.

On a peine à croire que, pour chaque demande nécessitant ces tâches de vérification et d'identification, un fonctionnaire de la Banque-Carrefour parcourt le site internet et les nombreuses autorisations des comités sectoriels pour s'assurer de la disponibilité de la donnée réclamée et de sa localisation dans le réseau. En outre, ces chemins informatiques peuvent certainement être copiés sur un document intelligible. En effet, lorsqu'une institution souhaite établir, avec la Banque-Carrefour, de nouveaux flux, des négociations s'engagent avec les comités sectoriels compétents et la Banque-Carrefour. Pour savoir qu'un nouveau flux est nécessaire et savoir sur quelles données il doit porter, les négociateurs doivent nécessairement être informés, par la Banque-Carrefour, des flux et des informations qui circulent déjà. À nouveau, on a peine à croire que cela ne peut se faire qu'en « déduisant » ces éléments du site internet et ce, en cours de réunion...

2. Une tâche disproportionnée pour le citoyen : la reconstitution du document. Dans son courrier, la Banque-Carrefour donne l'impression de réorienter le citoyen vers des documents pertinents dans lesquels il pourra aisément trouver réponse à ses questions. En accédant à ces liens internet, on s'aperçoit rapidement qu'il n'en est rien et que le citoyen pourrait même éprouver de l'humiliation en se retrouvant engouffré dans un tel amas d'informations complexes. En effet, les liens mentionnés renvoient à la description de l'ensemble des services de la Banque-Carrefour. À peu de choses près, il s'agit de l'ensemble du site internet. La toute grande majorité des informations accessibles n'ont aucun lien avec la table des données disponibles à laquelle il souhaite accéder. Si, face à ce constat, le citoyen ne perd pas courage, il essaiera de comprendre ce que signifie « formulaire électronique », et sera très déçu de ne pas en comprendre la définition[1087]. Plus encore, s'il souhaite dépouiller les décisions du Comité sectoriel de la sécurité sociale et de la santé, il risque d'éprouver de la stupeur en constatant que ce comité rend, en moyenne, 80 décisions par an depuis 1992. Dès lors, reconstituer la table des données disponibles à partir de ces documents exigerait plusieurs semaines, voire mois, de travail pour un chercheur travaillant dans cette matière.

La réponse de la Banque-Carrefour génère des interrogations fondamentales quant à la réalité du droit d'accès dans l'hypothèse qui vient d'être décrite.

Comment un citoyen, qui souhaiterait simplement savoir où vont être enregistrées les données qu'il accepte de communiquer à une institution,

[1087] En faisant une recherche par mot-clé, on aboutit à la définition suivante : Formulaire électronique : « Ensemble structuré de données destiné à l'échange électronique. Cette structure peut être décrite sur base de la syntaxe EDIFACT ou sous la forme d'un inhouse file normalisé ». Pour le reste, cette recherche par mot-clé renvoie à 8 pages de 8 occurrences chacune qui mentionnent les mots « formulaire électronique ».

pourrait-il trouver le courage et le temps pour reconstituer lui-même la table des données disponibles à partir des autorisations des comités sectoriels ?

La même question se pose pour un magistrat. On a vu précédemment[1088] que des institutions de sécurité sociale refusent l'octroi d'une aide à des citoyens dans le besoin, au motif qu'ils ne fournissent pas le document requis. Or, dans certains cas, ces institutions sont obligées de trouver par elles-mêmes les documents exigés, en passant par la Banque-Carrefour de la sécurité sociale. Un magistrat saisi d'un litige à ce sujet doit donc pouvoir vérifier si l'institution concernée est effectivement soumise à une telle obligation légale. Comment ce magistrat peut-il effectuer une telle vérification, s'il ne dispose d'une vision globale de quelles données sont accessibles à quelles institutions ?

Par ailleurs, comment admettre que des fonctionnaires de l'ONEm soient contraints de consacrer une partie importante de leur emploi du temps à reconstituer une base de données à partir des décisions de comités sectoriels alors que la Banque-Carrefour de la sécurité sociale pourra y parvenir aisément[1089] ?

On ne peut quand même pas exiger de chacun un travail d'une telle difficulté et d'une telle ampleur pour résoudre des questions relatives aux droits fondamentaux de tout administré.

Finalement, face à la réponse de la Banque-Carrefour de la sécurité sociale, nous avons introduit une demande d'avis auprès de la CADA. Elle s'est prononcée dans le sens de nos développements et le formule en ces mots : « La loi du 11 avril 1994 ne permet pas qu'une autorité administrative fédérale puisse se soustraire à une demande d'accès en renvoyant le demandeur aux pages du site Internet de l'autorité administrative fédérale concernée, parce que le citoyen a le libre choix d'en demander une copie. Par ailleurs il ne peut absolument pas être demandé au demandeur de faire l'effort de reconstituer le tableau sur la base d'informations tandis que la demande porte bien sur un document administratif existant. Il importe peu en effet que ce document soit sous format papier ou sou forme électronique. La Commission ne voit dès lors aucune raison de refuser de fournir une copie du document administratif demandé »[1090].

Depuis lors, la Banque-Carrefour de la sécurité sociale n'a pas réagi.

[1088] Voy. *supra,* n° 167.-

[1089] Voy. *supra,* n° 264.-

[1090] Commission d'accès aux documents administratifs, avis n° 2010-41 du 12 juillet 2010 sur le refus de donner accès à la table des données disponibles au sein du réseau sectoriel de la sécurité sociale.

3. Le document incompréhensible sans explications

300.- Le droit à des explications. Le citoyen qui recevrait un document administratif qu'il ne comprend pas a le droit d'obtenir des explications. En effet, le devoir de renseignement de l'administration est un « corollaire du droit constitutionnel d'accès »[1091], il en constitue un « complément naturel et indispensable »[1092]. La raison en est que, « dans la plupart des cas, la publicité sans explication resterait lettre morte en raison du caractère administratif du langage utilisé ou de la technicité des documents »[1093]. Cette affirmation est d'autant plus vraie aujourd'hui que l'administration est fondée sur des outils technologiques et recourt à des concepts informatiques que le citoyen a bien souvent du mal à comprendre sans être éclairé.

> Entre autres nombreux exemples, un citoyen essayant de comprendre ce qui est enregistré au Registre national trouvera des documents à ce sujet sur le site http://www.ibz.rrn.fgov.be. Parmi ces documents figure un dossier « Instructions pour la tenue à jour des informations », qui a été établi par le SPF Intérieur[1094]. Le citoyen pourrait s'étonner, en lisant la première page, de voir qu'un code N° 402b et un code N° 446 peuvent être utilisés pour indiquer des « remarques 'réfugié' ». En parcourant le document, il pourrait éprouver quelque difficulté de compréhension, raison pour laquelle un agent du registre national doit pouvoir lui fournir les explications dont il a besoin pour satisfaire à sa curiosité légitime.
>
> La même remarque a été faite à propos de la notion de « formulaire électronique » sur le site internet de la Banque-Carrefour de la sécurité sociale[1095].

301.- Le droit à des explications relatives aux outils informatiques. Il importe de souligner qu'à l'heure de l'électronique, le droit du citoyen d'obtenir des explications relatives aux documents administratifs impose aux agents de l'administration d'avoir certaines connaissances informatiques relatives aux outils qu'ils utilisent.

[1091] C.E., arrêt *de Liedekerke de Pailhe,* n° 112.495, du 12 novembre 2002 et arrêt *Roberti de Winghe et de Liedekerke*, n° 112.496, du 12 novembre 2002.

[1092] Projet de loi relatif à la publicité de l'administration, Rapport fait au nom de la commission de l'intérieur, des affaires générales et de la fonction publique par L. Peeters, *op. cit.,* p. 46.

[1093] Projet de loi relatif à la publicité de l'administration dans les provinces et les communes, Exposé des motifs, *Doc. Parl.,* Ch. Repr., sess. 1996-1997, n° 971/1, p. 6.

[1094] Ce document est disponible à l'adresse suivante : http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Registre/fr/instructions/instructions.pdf

[1095] Voy. *supra,* n° 299.-

En effet, comme dit précédemment, un logiciel détenu par une administration est un document administratif. Un citoyen pourrait donc légitimement réclamer des explications sur les modalités de fonctionnement de celui-ci, ses composantes, voire son code source. Cela signifie que l'administration doit veiller à former des agents capables de fournir ces explications techniques[1096].

II. La publicite active confrontée à l'e-gouvernement

302.- La notion de publicité active. La publicité active vise la communication d'informations à la population de la propre initiative des administrations[1097]. En d'autres termes, il s'agit, pour les administrations, de faire connaître les informations qu'elles détiennent, d'exposer les axes majeurs des politiques menées, de détailler les compétences de leurs services, et ce, sans attendre la demande d'accès d'un administré.

La loi du 11 avril 1994 impose aux autorités administratives fédérales le respect de quelques obligations se rattachant à la publicité active. Comme le prévoit l'article 2 de la loi d'accès, il s'agit de « fournir une information claire et objective sur l'action des autorités administratives fédérales ». Malheureusement, ces obligations sont limitées. Des améliorations sont nécessaires.

A. Des obligations limitées

303.- L'institution d'un service d'information fédéral. La loi du 11 avril 1994 délègue au Roi la compétence d'organiser un service d'information fédéral, d'en déterminer l'organisation et d'en détailler les missions[1098]. En somme, il revient à ce service de déterminer la politique d'information menée au sein des administrations fédérales, et de guider le citoyen dans l'identification de l'administration à laquelle il doit s'adresser[1099].

[1096] Pour de plus amples développements à ce sujet, en lien notamment avec les marchés publics, D. De Roy, « L'accès aux documents administratifs dans un environnement dématérialisé », *op. cit.,* pp. 849 à 851.

[1097] Projet de loi relatif à la publicité de l'administration, Exposé des motifs, *op. cit.,* p. 12.

[1098] Art. 2, 1°, de la loi du 11 avril 1994.

[1099] Projet de loi relatif à la publicité de l'administration, Rapport fait au nom de la Commission de l'intérieur, des affaires générales et de la fonction publique, *op. cit.,* p. 42. Remarquons que le législateur a donc laissé au pouvoir exécutif le soin de décider librement du contenu des informations communiquées et des moyens techniques utilisés pour ce faire. On peut ainsi « légitimement craindre que les choix opérés dans l'information ne soient

À l'époque de l'entrée en vigueur de la loi, l'Institut belge d'Information et de Documentation (Inbel) œuvrait déjà en ce domaine. La mission du Roi s'est réduite à rebaptiser cet organisme en « Service Fédéral belge d'Information »[1100] (SFI). En juillet 2003, le SFI a été dissout et ses missions en matière de publicité active ont été transférées au service public fédéral Chancellerie du Premier Ministre[1101], qui assure encore ces missions aujourd'hui[1102].

304.- La publication de guides. La loi impose à chaque autorité administrative de rédiger un document précisant ses compétences et son organisation interne. Grâce au développement de l'Internet, la plupart de ces guides sont désormais disponibles en ligne, sur le site de chaque administration. Certaines administrations ont utilement intégré dans ces guides des explications relatives aux évolutions que leurs services connaissent dans le contexte de l'e-gouvernement.

> Par exemple, le site du SPP Intégration sociale contient une rubrique « *E-government et applications du Web* » qui fournit des explications relatives à l'intégration de cette administration dans le réseau de la sécurité sociale, à l'existence d'échanges de données avec d'autres services publics, etc.[1103].

305.- La publicité dans les documents individuels. Chaque document que l'administration fait parvenir au citoyen doit mentionner *le nom et les coordonnées du fonctionnaire en charge du dossier*[1104]. Ce faisant, la personne concernée souhaitant obtenir des informations sur son dossier trouvera plus aisément l'interlocuteur compétent pour la renseigner.

Bien que la loi n'impose que d'indiquer le nom, la qualité, l'adresse et le numéro de téléphone du fonctionnaire pouvant fournir des informations relatives au dossier, de plus en plus d'administrations mentionnent

---

guidés par un souci sinon propagandiste, du moins justificateur des politiques menées » (C. DE TERWANGNE, *Société de l'information et mission publique d'information, op. cit.,* p. 250, n° 211. Voy. égal. pp. 362 et s.)

[1100] Arrêté royal du 30 mai 1994 modifiant la dénomination de l'établissement d'utilité publique « Inbel, Institut belge d'Information et de Documentation », en « Le Service Fédéral belge d'Information – SFI », *M.B.,* 29 juin 1994, err. *M.B.,* 17 novembre 1994.

[1101] Arrêté royal du 3 mai 2003 relatif à la dissolution du Service fédéral belge d'Information et au transfert des biens, droits et obligations au Service public fédéral Chancellerie du Premier Ministre et au Service public fédéral Affaires étrangères, Commerce extérieur et Coopération au Développement, *M.B.,* 26 mai 2003.

[1102] Voy. le site http://www.chancellerie.belgium.be

[1103] Voy. http://www.mi-is.be/be-fr/e-government-et-applications-web/e-government-et-applications-web

[1104] Art. 2, 3°, de la loi du 11 avril 1994.

également le courriel. On doit y voir la possibilité, pour l'administré, de dialoguer avec l'administration par voie électronique, même si la loi d'accès ne le prévoit pas expressément[1105].

En outre, tout document notifiant une décision ou un acte administratif à portée individuelle doit mentionner les *voies éventuelles de recours*, ainsi que les formes et les délais à respecter. Seule cette obligation est assortie d'une sanction : à défaut pour l'autorité de respecter ce prescrit, le délai de prescription pour introduire le recours ne prend pas cours[1106].

B. Des améliorations nécessaires

306.- L'utilité de la publicité active pour les administrations et les citoyens. Il est regrettable que la publicité active n'ait pas fait l'objet de plus d'attention de la part du législateur.

En effet, loin de n'être qu'une charge supplémentaire pesant sur les administrations, elle leur offre des avantages. En diffusant spontanément certaines informations, l'administration fait des économies de moyens, étant dispensée de répondre maintes fois à des demandes portant sur le même document[1107]. En outre, une publicité active développée témoigne de la bonne volonté des institutions publiques, incitant davantage les citoyens à la confiance[1108].

Par ailleurs, la publicité active épargne aux citoyens la tâche, de plus en plus complexe, de déterminer et de solliciter eux-mêmes les informations recherchées. Elle améliore ainsi l'égalité entre les administrés, « puisque l'accès à l'information n'est plus tributaire de la connaissance préalable, et parfois aléatoire, de son existence : tous les administrés y ont automatiquement accès, en principe sous la même forme et aux mêmes conditions »[1109].

[1105] D. De Roy, « L'accès aux documents administratifs dans un environnement dématérialisé », *op. cit.,* p. 839.

[1106] Art. 2, 4°, de la loi du 11 avril 1994. Pour des applications jurisprudentielles, voy. C. Doyen-Biver, « La législation sur l'accès aux documents administratifs. Aperçu de ses applications », *in Transparence et droit à l'information, op. cit.,* pp. 32-34.

[1107] D. De Roy, « L'accès aux documents administratifs dans un environnement dématérialisé », *op. cit.,* p. 846 ; R. Andersen, « Conclusions générales », *in L'accès aux documents administratifs* (dir. D. Renders), *op. cit.*, p. 956 ; J. Laveissière, « L'accès aux documents administratifs », *op. cit.*, p. 24.

[1108] R. Andersen, « Conclusions générales », *in L'accès aux documents administratifs* (dir. D. Renders), *op. cit.*, p. 956 ; F. Rangeon, « L'accès à l'information administrative », *in Information et transparence administratives*, *op. cit.,* p. 95.

[1109] *Idem*. Dans le même sens, J. Laveissière, « L'accès aux documents administratifs », *op. cit.*, p. 25.

307.- L'utilité particulière de la publicité active dans l'e-gouvernement. Le développement de l'e-gouvernement rend nécessaire le déploiement de la publicité active. En effet, les évolutions considérables que connaît aujourd'hui l'administration dans sa structure et son fonctionnement doivent être communiquées et expliquées aux administrés, de manière claire et compréhensible. À partir du moment où l'administration utilise des nouvelles méthodes de travail grâce aux traitements de bases de données, il faut lui imposer de nouvelles obligations de transparence[1110]. Comme l'ont montré les développements qui précèdent, « la vieille logique du droit d'accès »[1111] ne suffit plus. Elle doit être dépassée.

Un tel changement est d'autant plus justifié qu'il est techniquement possible aujourd'hui et ne constitue plus un frein à l'efficacité administrative, vu les facilités qu'offrent les technologies[1112]. Plus encore, l'administration peut s'appuyer sur l'utilisation d'Internet qui, grâce à sa rapidité et son rayonnement illimité, donne un grand impact à la diffusion d'informations sur la toile et répond pleinement à l'idéal de transparence[1113]. On peut ainsi affirmer que « l'état de la technique permet [...] d'imposer à l'administration une obligation à caractère général », celle de « diffuser toute l'information et toutes les données disponibles »[1114].

Le législateur devrait donc définir de manière claire et cohérente, des obligations de publicité active adaptées à l'e-gouvernement.

C'est en ce sens qu'a déjà agi le législateur en matière de publicité des informations environnementales. La directive européenne adoptée en la matière[1115], ainsi que la loi belge qui la transpose en droit belge[1116] promeuvent le développement de la publicité active et encourage, pour ce faire, l'utilisation des technologies de l'information et de la communication. Il est affirmé explicitement que la diffusion de l'information en matière d'environnement favorise « une plus grande sensibilisation aux questions d'environnement, le libre échange d'idées, une participation

---

[1110] E. Malaret, « Droit, administrations publiques et NTIC : vers la restructuration de l'espace public. Les instruments pour la construction d'une démocratie dialogique », *in Études en l'honneur de Gérard Timsit,* Bruxelles, Bruylant, 2004, p. 428.

[1111] *Idem.*

[1112] Voy. *infra,* n° 382.-

[1113] D. De Roy, « L'accès aux documents administratifs dans un environnement dématérialisé », *op. cit.,* p. 847.

[1114] E. Malaret, *op. cit.,* p. 428.

[1115] Directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement, *J.O.U.E.,* 14 février 2003, L 41/26.

[1116] Loi du 5 août 2006 relative à l'accès du public à l'information en matière d'environnement, *M.B.,* 28 août 2006, p. 42538.

plus efficace du public à la prise de décision en matière d'environnement »[1117].

Dans l'attente d'une intervention législative concernant les informations administratives en général, rien n'empêche l'administration de développer des initiatives en matière de publicité active, dans son intérêt, et celui des administrés. Plus particulièrement, il conviendrait d'améliorer la communication administrative institutionnelle et la communication administrative informative.

§1. L'amélioration de la communication administrative institutionnelle

308.- Les difficultés liées à une publicité active en silos. La communication administrative institutionnelle vise la diffusion des informations « portant sur les services et les activités des institutions »[1118].

Pour l'heure, conformément à la loi, chaque administration assure la publicité active qui la concerne. La communication institutionnelle est donc éparpillée sur le site internet des multiples administrations du pays. Sans surprise, cette compartimentation des informations correspond à la structure de l'administration en silos, par rapport à laquelle a été pensée la loi d'accès. Dès lors, aujourd'hui, on peine à trouver trace d'explications propres à l'e-gouvernement, faisant notamment état du regroupement d'administrations au sein de réseaux.

Plus particulièrement, il manque un panorama général qui mentionnerait les réseaux sectoriels déjà en place, les administrations qui en font partie, les sources authentiques de données existantes et les types de données enregistrées dans celles-ci ainsi que les échanges de données autorisés. De toute évidence, un tel outil contribuerait à « vulgariser par tous les vecteurs de communication adéquats les axes majeurs » de la politique des services publics, comme l'y invite la Charte de l'utilisateur des services publics[1119].

> Par exemple, certaines administrations évoquent, sur leur site internet, leur appartenance au réseau sectoriel de la sécurité sociale. À partir de là, un citoyen peut effectuer des recherches qui l'amèneront au site de la Banque-Carrefour de la sécurité sociale. En parcourant ce portail, il finira par cliquer sur « la BCSS en bref » et trouver une explication de cette structure nouvelle

[1117] Considérant 1 de la directive 2003/4/CE précitée. Voy. égal. Projet de loi relatif à l'accès du public à l'information en matière d'environnement, Exposé des motifs, *op. cit.*, p. 6.

[1118] C. de Terwangne, *Société de l'information et mission publique d'information*, *op. cit.*, p. 383, n° 384.

[1119] Chapitre 1er, 1, de la Charte de l'utilisation des services publics du 4 décembre 1992.

de l'administration. Ces informations sont néanmoins limitées au domaine de la sécurité sociale.

Le SPF Fedict est un SPF dit « horizontal », chargé notamment d'assister les autres services publics pour les aider à s'adapter aux nouveautés liées à l'e-gouvernement. On trouve donc sur leur site internet des informations faisant état de ces avancées, d'un point de vue global. Malheureusement, le langage utilisé est, à certains égards, complexe, et les informations semblent sommaires. Par exemple, en cliquant sur la rubrique « échange de données », on voit apparaître une explication des données à caractère personnel qui se résume à dire que « les services web permettent de rechercher des données à caractère personnel dans le Registre national ou de rechercher et mettre à jour ce type de données dans le Registre Bis ». Il existe pourtant bien d'autres données à caractère personnel utilisées… Par ailleurs, ce site semble s'adresser davantage aux administrations souhaitant mettre en place de nouveaux services informatiques, qu'aux citoyens désireux de comprendre le contexte administratif nouveau qui les entoure.

§2. L'amélioration de la communication administrative informative

309.- Considérations générales. La communication administrative informative consiste en « la diffusion d'informations sur les décisions prises, sur les règlementations en vigueur ou nouvelles, […] »[1120].

En ce qui concerne plus particulièrement l'e-gouvernement, on se concentre sur les améliorations qui pourraient être apportées aux les informations relatives aux droits des citoyens, aux outils nouveaux et aux données traitées.

310.- La communication relative aux droits des citoyens. Contrairement à la communication institutionnelle qui vient d'être abordée, la publicité des services offerts aux citoyens fait déjà l'objet d'initiatives intéressantes de la part des pouvoirs publics. Celles-ci se basent sur les possibilités nouvelles offertes par les technologies, notamment en termes d'échanges de données entre administrations. Elles sont également disponibles en ligne.

Par exemple, on souligne l'intérêt du site www.belgium.be, géré par la Chancellerie du Premier Ministre[1121]. Ce portail internet regroupe tous les services en ligne qu'offrent les services publics aux citoyens et aux entreprises

[1120] C. DE TERWANGNE, *Société de l'information et mission publique d'information*, *op. cit.*, p. 386, n° 388.

[1121] Rappelons que la Chancellerie du Premier Ministre assure le rôle de service d'information fédéral central, *in*stitué par la loi du 11 avril 1994.

belges. Trois classements sont disponibles, pour accéder plus aisément à ce que l'on recherche : un classement par thème (justice, famille, impôts, etc.), un classement par niveau de pouvoir (fédéral, communautaire, régional, provincial) et un classement des applications qui nécessitent l'utilisation de la carte d'identité électronique.

Signalons toutefois que des améliorations pourraient utilement être apportées à ce portail, pour en faciliter l'usage. Il est par exemple regrettable de s'apercevoir que les parents d'un enfant handicapé sont renvoyés vers un document PDF de 108 pages lorsqu'ils veulent simplement connaître le montant de l'allocation à laquelle leur enfant a droit et le service auquel ils doivent s'adresser pour obtenir cette aide.

Pour améliorer ce portail, on pourrait s'inspirer du portail français www.service-public.fr. Il reprend, sur une interface moderne et éthérée, 10 rubriques correspondant aux problématiques administratives des citoyens. Concernant plus particulièrement l'octroi d'allocations, ce site contient un outil de recherche permettant de trouver, à partir de son code postal, l'organisme compétent le plus proche.

De toute évidence, une telle informatisation des démarches administratives est de nature à faciliter la tâche du citoyen, qui ne doit plus se déplacer ni se soumettre à des horaires stricts, et encore moins patienter devant un guichet.

Néanmoins, ces démarches supposent que les administrés aient connaissance des droits et obligations qui sont les leurs. Ces obligations leur sont en général rappelées par l'administration compétente en temps utile. Par contre, les individus n'ont pas toujours connaissance des droits qui leur sont offerts. Ils peuvent alors ignorer l'existence d'une allocation qui s'adresse à eux, ou la possibilité d'obtenir une réduction de certaines taxes, etc. Or, des outils existent aujourd'hui, qui permettent de pallier cette difficulté.

Ainsi, pour contrer cette ignorance, le développement de l'e-gouvernement permet d'automatiser de plus en plus de droits. Néanmoins, comme en a fait état le premier titre de cette recherche, une telle automatisation suppose de nombreux échanges de données à caractère personnel et pose question au regard de la protection de la vie privée des personnes concernées.

C'est pourquoi, la mise en place, par le Gouvernement flamand, d'un *Rechtenverkenner*[1122] (« explorateur de droits ») est une initiative particulièrement enthousiasmante. Cet outil permet au citoyen d'obtenir un aperçu des droits auxquels il peut prétendre. À partir de là, il est libre d'effectuer, ou non, les démarches nécessaires, en gardant la maîtrise des données qu'il choisit de communiquer, ou non, à l'autorité compétente.

[1122] Cet outil est disponible sur le site http://www.rechtenverkenner.be

L'explorateur de droit a été institué par un décret flamand du 23 décembre 2010[1123] qui le définit comme « un instrument pour la recherche de droits », comprenant « un aperçu de mesures prises par les différentes autorités afin de réaliser les droits du citoyen » en matière économique et sociale.

Grâce à cet outil, le citoyen peut « créer un aperçu personnalisé de droits pertinents ». Pour ce faire, l'explorateur de droits se fonde sur une utilisation maximale des données à caractère personnel de l'utilisateur détenues par les autorités. Néanmoins, cette utilisation est très encadrée et temporaire. Ainsi, le citoyen doit autoriser la collecte et le traitement des données. En outre, ne sont utilisées que les données nécessaires pour créer l'aperçu des droits du citoyen. Plus encore, « l'explorateur de droits ne peut pas conserver ces données à caractère personnel au-delà du temps nécessaire pour l'établissement d'un aperçu personnalisé des droits »[1124]. En somme, grâce à cet outil, le citoyen peut agir de manière proactive, en vérifiant à quels droits il peut prétendre. La CPVP s'est montrée favorable à ce décret[1125].

311.- La communication relative aux outils nouveaux et aux règles qui s'y appliquent. Comme on l'a déjà souligné, il est difficile d'accéder aux informations éclairant le fonctionnement des outils nouveaux qui fondent l'e-gouvernement ainsi que l'interprétation des règles qui s'y appliquent.

> En guise d'exemple de ces difficultés, on rappelle nos démarches effectuées auprès du Comité sectoriel sécurité sociale pour obtenir une copie de l'étude expliquant le fonctionnement de l'entrepôt de données OASIS. L'exercice de notre droit d'accès s'apparente à un parcours du combattant compte tenu des multiples exceptions qui ont été invoquées par cette administration[1126].

Pourtant, ces informations existent. Au gré de l'accomplissement de leurs tâches, la CPVP, les comités sectoriels, les plateformes d'échanges d'information acquièrent une expertise indéniable dans leur sphère d'activité. Celle-ci se manifeste dans des documents que ces organes rédigent : des analyses faisant le point sur une jurisprudence, des rapports étudiant les questions suscitées par une évolution technologique, etc. De plus, le travail de ces experts est bien souvent réalisé à la lumière d'études et de rapports destinés à éclairer les décideurs en leur

[1123] Décret flamand du 23 décembre 2010 relatif à l'explorateur de droit (*rechtenverkenner*), *M.B.*, 17 mars 2011.

[1124] Art. 2 dudit décret.

[1125] CPVP, avis n° 03/2010 du 3 février 2010 concernant l'avant-projet de décret modifiant le décret du 19 mars 2004 relatif à la politique sociale locale.

[1126] Voy. *supra*, n^{os}289.- et s.

expliquant notamment comment fonctionnent les outils au sujet desquels ils doivent se prononcer. Malheureusement, actuellement, peu de ces documents sont publiés.

> Ainsi, par exemple, la CPVP publie un rapport d'activité annuel. Néanmoins, celui-ci ne constitue qu'une synthèse des « principales activités » de la CPVP et des comités sectoriels, selon les termes utilisés par ces rapports. En outre, les avis de cette Commission et les autorisations des comités sectoriels sont disponibles sur le site internet www.privacycommission.be. Malheureusement, ils sont extrêmement nombreux et leur lecture est fastidieuse. C'est probablement la raison pour laquelle la CPVP, notamment, élabore des analyses de ces décisions et avis. Celles-ci ne sont toutefois pas publiées. Par ailleurs, aucune base de données ne recense les rapports, études, tableaux de synthèse soumis aux membres de ces organes institutionnels dans l'exercice de leurs tâches. Ce manque de transparence est d'autant plus étonnant que la CPVP entend « faire en sorte que les acteurs – publics et privés – ayant recours [aux] technologies aient une vision claire des droits fondamentaux des citoyens ; veillent à respecter et à faire respecter ces droits ; prennent les mesures concrètes propres à garantir la sécurité de l'information et la préservation de la vie privée des citoyens »[1127].
>
> Le manque d'informations livrées apparaît de manière plus évidente encore si l'on compare le site internet de la CPVP au portail du Bureau du plan[1128]. Le Bureau du plan et la CPVP ont ceci en commun d'être chargés d'éclairer le public quant aux conséquences des choix politiques, le premier pour les questions économiques et sociales[1129], la seconde, on l'a dit, en ce qui concerne la protection de la vie privée des citoyens. La communication des informations dont dispose le Bureau du plan est particulièrement généreuse. Ainsi, sont disponibles sur le site internet www.plan.be, les « working papers » – reprenant des analyses menées au sein de l'institution – les exposés, les rapports annuels, les bulletins trimestriels – faisant le point sur les études en cours, les décisions récentes, certaines questions d'actualité – ainsi que nombre d'études réalisées et de tableaux d'analyses dressés.

Néanmoins, cette problématique semble retenir actuellement l'attention des pouvoirs publics, si bien que l'on peut espérer prochainement une ouverture progressive des données administratives.

Ainsi, des nouveautés sont à prévoir en Flandre. Le Gouvernement flamand a en effet approuvé, le 23 septembre 2011, la note conceptuelle

---

[1127] Extrait de la page du portail de la Commission de la protection de la vie privée consacrée à la « vision » de cette institution en ce qui concerne son rôle. http://www.privacycommission.be/fr/commission/about/vision/

[1128] www.plan.be

[1129] Art. 127 de la loi du 21 décembre 1994 portant des dispositions sociales et diverses, *M.B.,* 23 décembre 1994, p. 31878.

de son ministre des affaires administratives, Geert Bourgeois, relative aux « open data »[1130]. Selon cette note, il importe de s'engager plus franchement dans l'ouverture des données publiques notamment en créant un registre central des données disponibles et en publiant des données issues de sources authentiques, dans la mesure où cette publication ne porte pas atteinte à la vie privée des citoyens, notamment. Le lien entre la transparence et le bon développement de l'e-gouvernement est explicitement affirmé, la note soulignant que « de opmaak van een interbestuurlijke diensten – en productencatalogus, een gestandaardiseerde en gestructureerde beschrijving van het aanbod van Vlaamse overheden, is een bouwsteen voor een geïntegreerde overheid ».

Quelques jours plus tard, le 28 septembre 2011 a été inauguré le site www.data.gov.be. Il s'agit d'un portail internet regroupant des ensembles de données provenant des différentes administrations du pays, géré par le SPF Fedict. Pour l'heure, ce site ne contient pas beaucoup de données, mais il est appelé à se développer. En ce qui concerne plus particulièrement l'e-gouvernement, il pourrait être judicieux d'insérer sur ce site un index des documents et études existant au sein des différentes administrations. Cet index permettrait au citoyen de prendre aisément connaissance des documents existants en ce domaine. La faiblesse évidente de cet outil d' « open data » est sa dépendance par rapport au bon vouloir des SPF, qui décident seuls des informations qu'ils acceptent de livrer. À nouveau, une intervention du législateur en matière de publicité active ne serait pas inutile…

Plus encore, le 12 décembre 2011, la Commission européenne a présenté une « stratégie européenne en matière d'ouverture des données publiques »[1131] dans laquelle elle insiste sur l'importance d'assurer la transparence du fonctionnement du secteur public à l'égard des citoyens, présente des exemples de bonnes pratiques et suggère notamment une révision de la directive 2003/98/CE sur la réutilisation des données du secteur public[1132].

312.- La communication relative aux données à caractère personnel traitées. Les données à caractère personnel des citoyens constituent un matériau de base de l'e-gouvernement car, en vertu du principe de la collecte unique des données, ces informations ont vocation à être réutilisées un grand nombre de fois. Ces données doivent donc être exactes,

[1130] Conceptnota aan de Vlaamse Regering bettreffende een concept van beleid met betrekking tot open data. La note est disponible sur le site http://bestuurszaken.be/

[1131] COM(2011)882, 12 décembre 2011, Open data, an engine for innovation, growth and transparent development.

[1132] À ce sujet, voy. A.M. Klingenberg, « Gefragmenteerde openheid : open data, Europa, en de Wob », *Computerrecht,* 2012, liv. 5, pp. 331 à 338.

ce qui relève de la responsabilité des détenteurs de sources authentiques, comme l'a souligné le premier titre de la recherche.

Pour s'assurer de la qualité des données utilisées, il peut être judicieux, pour l'administration qui détient ces informations, de contacter, à intervalles réguliers, les personnes concernées en leur demandant si les données détenues à leur sujet sont encore à jour. Cela peut se faire en envoyant aux citoyens une copie des données détenues à leur sujet. Une telle démarche peut être qualifiée de publicité active individuelle.

Malheureusement, la loi du 11 avril 1994 ne fait aucune allusion à l'utilisation des données à caractère personnel dans les administrations et à l'importance d'un dialogue à ce sujet avec les personnes concernées. Etant donné que cette loi est postérieure à la loi du 8 décembre 1992 sur les traitements de données à caractère personnel, on aurait pu raisonnablement espérer un lien explicitement affirmé avec cette législation particulière. Celle-ci prévoit en effet certaines règles de publicité active. Elles seront étudiées au chapitre suivant.

Section 3. Le droit de comprendre ébranlé par l'e-gouvernement

313.- Considérations générales. Comme on l'a mentionné précédemment, la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs impose aux autorités administratives d'indiquer explicitement dans l'acte les raisons qui fondent celui-ci[1133].

L'obligation de motivation satisfait ainsi à divers objectifs.

Le citoyen est en mesure de comprendre les raisons qui ont amené l'administration à lui imposer tel montant d'impôts ou à lui octroyer telle allocation, par exemple. À cette occasion, il peut contrôler l'exactitude des motifs sur lesquels se fonde l'autorité et les contester, le cas échéant.

En outre, une telle obligation incite l'administration à adopter des décisions rigoureuses et objectivement justifiables, sans céder à la tentation de l'arbitraire.

[1133] Le droit de comprendre est utilisé ici comme le droit, pour un citoyen, de comprendre les décisions administratives qui le concernent. On a vu précédemment que la loi du 11 avril 1994 consacre le droit obtenir des explications, qui est donc également un « droit de comprendre » relatif aux documents administratifs en général et est un corollaire du droit d'accès aux documents administratifs. Il a été étudié précédemment (Voy. *supra,* n° 300.-).

Enfin, l'obligation de motivation aide également les autorités de contrôle dans leur examen de la légalité des décisions administratives[1134].

À l'heure où beaucoup de décisions administratives sont prises à partir de traitements de données à caractère personnel, le citoyen est-il encore en mesure de comprendre le raisonnement de l'autorité administrative ?

Parmi les conditions d'applicabilité de la loi du 29 juillet 1991, deux d'entre elles posent particulièrement question dans l'e-gouvernement.

La première condition vise l'acte à motiver.

La seconde condition concerne le contenu de la motivation[1135].

I. L'acte à motiver

314.- Un acte juridique, unilatéral, de portée individuelle : une exigence mal adaptée. L'article 1er de la loi soumet à l'obligation de motivation « l'acte juridique unilatéral de portée individuelle émanant d'une autorité administrative et qui a pour but de produire des effets juridiques à l'égard d'un ou de plusieurs administrés ou d'une autre autorité administrative ».

L'*acte juridique* est un acte « posé délibérément en vue de créer des effets juridiques ou d'empêcher que certains effets juridiques ne se produisent »[1136]. Pour le dire autrement, ne sont visés par la loi que les décisions administratives ayant pour but de modifier une situation juridique ou, au contraire, d'en empêcher la modification. Par contre, les actes matériels ou de pur fait, ainsi que les actes préparatoires à une décision, ne constituent pas des actes juridiques[1137].

[1134] SLCE, avis du 21 octobre 1987 relatif à la proposition de loi relative à la motivation formelle des actes administratifs, *Doc. Parl.,* Sénat, sess. extr. 1988, n° 215-2, p. 6 ; Rapport fait au nom de la Commission de l'Intérieur par M. Flagothier, *Doc. Parl.,* Sénat, sess. Extr. 1988, n° 215-3, pp. 2, 3 et 10 ; D. Lagasse, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs », *J.T*, 1991, p. 737 ; M. Maerevoet, *La motivation formelle des actes administratifs en matière de marchés publics*, Bruxelles, Larcier, 2011, pp. 19-22.

[1135] L'art. 2 de loi du 29 juillet 1991 impose également des limites quant à l'autorité soumise à l'obligation, qui doit revêtir la qualité d'autorité administrative. L'art. 4 de cette loi prévoit également un certain nombre d'exceptions à l'obligation de motivation. Néanmoins, ces limites classiques ne semblent pas amplifiées par l'e-gouvernement. C'est la raison pour laquelle nous ne les étudions pas dans le cadre de cette recherche.

[1136] Rapport fait au nom de la Commission de l'Intérieur par M. Flagothier, *op. cit.,* n° 215-3, p. 29.

[1137] R. Andersen et P. Lewalle, « La motivation formelle des actes administratifs », *A.P.T.*, 1993, p. 67 ; J. Salmon, *Le Conseil d'État,* t. I, Bruxelles, Bruylant, 1994, p. 274 ; P. Lewalle, *Contentieux administratif*, *op. cit.,* pp. 248à 250 ; I. Opdebeek et A. Coolsaet, *Formele motivering van bestuurshandelingen*, Brugge, die Keure, 1999, pp. 168-169 ; M. Maerevoet, *op. cit.,* p. 65.

L'*acte unilatéral* émane de la seule volonté de l'administration. Il s'oppose aux contrats administratifs, qui résultent d'un échange de consentement et échappent à l'obligation de motivation[1138].

L'*acte de portée individuelle* s'adresse à un ou plusieurs destinataires, dont le nombre est déterminé ou du moins, déterminable. Il s'oppose au règlement qui revêt un caractère général et abstrait. Ce dernier est exclu du champ d'application de la loi[1139].

315.- L'acte juridique dans l'e-gouvernement. Parmi les exigences qui conditionnent l'obligation de motivation, celle d'un « acte juridique » est mal adaptée à l'e-gouvernement et limite particulièrement le droit de comprendre dans ce contexte.

En effet, on sait à présent que de nombreuses décisions administratives sont fondées sur des traitements de données qui ont lieu en amont et prennent notamment la forme de transferts de données entre administrations.

La décision administrative finale, qui a été prise à partir de ces traitements de données, est un acte juridique. Elle doit donc être motivée.

En revanche, les traitements de données qui ont permis de prendre cette décision échappent à cette obligation de motivation. Ces traitements de données doivent, en effet, être qualifiés de « mesures préparatoires » des décisions futures, qui n'apportent en principe, par eux-mêmes, aucune modification à une situation juridique existante. On peut comparer les transferts de données, aujourd'hui, aux transferts de dossiers papier, hier. Or, ces derniers ont jadis été reconnus comme des agissements matériels ne constituant pas des actes juridiques et échappant, de ce fait, à l'obligation de motivation[1140].

Dès lors, puisque les traitements de données ne sont pas soumis à l'obligation de motivation, le citoyen qui apprend que des échanges de données ont eu lieu pour prendre la décision administrative finale ne peut pas invoquer la loi du 29 juillet 1991 pour exiger de savoir qui a utilisé ses données, pour quelle raison, de quelle source provenaient-elles,

---

[1138] Rapport fait au nom de la Commission de l'Intérieur par M. Flagothier, *op. cit.,* n° 215-3, p. 30 ; X. Delgrange et B. Lombaert, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : questions d'actualité », *op. cit.,* pp. 30 et 31.

[1139] X. Delgrange et B. Lombaert, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : questions d'actualité », *op. cit.,* pp. 31-33 et les références citées.

[1140] C.E., *Damsaint,* n° 1354, du 7 mars 1952, cité par J. Salmon, *Le Conseil d'État, op. cit.,* p. 266. Dans cet arrêt, il était question de la communication, par le Procureur du Roi, à un Bourgmestre, d'un dossier d'information à charge d'un agent de la police communale.

et corollairement, il ne peut vérifier la légalité de l'action administrative et l'exactitude des données échangées. Le droit de comprendre du citoyen, censé être assuré par la loi du 29 juillet 1991, est affecté dans l'e-gouvernement.

> Par exemple, un fonctionnaire décide de contrôler un employeur suspecté de fraude car plusieurs alarmes se sont mises en route dans l'entrepôt de données OASIS. Cet employeur ne peut pas exiger de connaître les traitements de données effectués pour aboutir à la décision de le contrôler car l'utilisation d'OASIS et la décision de contrôler cet employeur constituent des mesures préparatoires à une éventuelle sanction[1141].

II. Le contenu de la motivation

316.- Des exigences mal adaptées et mal appliquées. Parmi les exigences relatives au contenu de la motivation d'un acte administratif, certaines sont mal adaptées à l'e-gouvernement. D'autres sont intéressantes mais s'avèrent mal appliquées. Elles gagneraient à être interprétées autrement dans ce contexte nouveau.

317.- Motivation de droit et de fait. Il ressort de l'article 3 de la loi du 29 juillet 1991 que « la motivation exigée consiste en l'indication, dans l'acte, des considérations de droit et de fait servant de fondement à la décision. Elle doit être adéquate ».

Comme l'explique Dominique Lagasse, la motivation formelle d'un acte administratif consiste à exposer à la personne concernée « dans la décision elle-même le raisonnement en droit et en fait qui lui sert de fondement [...] Elle permet au citoyen, destinataire de la décision, de comprendre la portée de celle-ci : le document qui porte la décision à sa connaissance doit à cet effet énoncer expressément les motifs qui ont conduit à la décision. Ceux-ci doivent en outre figurer dans le dossier administratif »[1142].

En particulier, la motivation *en droit* consiste à mentionner le fondement juridique en vertu duquel l'acte a été adopté. En d'autres termes,

---

[1141] À ce sujet, voy. not. C.E., *SA Falkenberg et fils,* n° 60.062 du 17 juillet 1996, p. 3 (concernant le fait que la décision de contrôler un citoyen est une mesure préparatoire) ; C.E., *Brauwers,* n° 91.994, 8 janvier 2001, p. 5 (qui affirme qu'un acte préparatoire n'est pas soumis à l'obligation de motivation formelle).

[1142] D. Lagasse, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs. Incidences en droit social », *Orientations,* 1993, p. 68.

il s'agit d'indiquer la base légale qui fonde la compétence de l'auteur de l'acte.

La motivation *en fait* consiste à indiquer les circonstances concrètes qui ont amené l'autorité à adopter l'acte administratif. Elle doit être adéquate, c'est-à-dire « claire, précise, complète et véritable »[1143] car « le citoyen qui fait l'objet d'une décision doit connaître les éléments qui lui permettent de comprendre exactement la portée »[1144] de celle-ci.

Dans l'e-gouvernement, la motivation en fait de décisions prises à partir de traitements de données est particulièrement délicate pour plusieurs raisons qu'on détaille à présent.

318.- E-gouvernement et traitements de données à caractère personnel. Etant donné la mise en œuvre du principe de la collecte unique des données, nombre de décisions administratives sont prises à partir de traitements de données effectués préalablement. Néanmoins, l'administration n'est pas tenue de mentionner, dans sa décision, l'existence de tels traitements. Elle doit, en effet, mentionner les données qui permettent au citoyen de comprendre la décision prise, mais non la manière dont ces informations ont été obtenues.

> Par exemple, le SPF Economie reçoit du SPF Finances l'information selon laquelle tel demandeur de l'allocation de chauffage dépasse, oui ou non, le seuil de revenus en dessous duquel l'allocation peut être octroyée. Quand le SPF Economie notifie sa décision à la personne concernée, il se contente de dire que l'allocation de chauffage est refusée au motif que le seuil de revenu est dépassé. La loi du 29 juillet 1991 ne l'oblige pas à indiquer d'où provient l'information selon laquelle le seuil est dépassé.

Pour pallier cette lacune, la loi devrait prévoir l'obligation de mentionner, dans la décision administrative, un certain nombre d'indications sur les traitements de données ayant permis de rendre cette décision.

La loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale prévoyait pareille obligation il y a quelques années. Malheureusement, cette obligation a été supprimée depuis lors.

a) L'ancien article 20 de la loi sur la Banque-Carrefour de la sécurité sociale. Dans sa version initiale, la loi du 15 janvier 1990 sur la

[1143] Proposition de loi relative à la motivation formelle des actes administratifs, Développements, *op. cit.,* p. 9.

[1144] Rapport fait au nom de la Commission de l'Intérieur par M. Flagothier, *op. cit.,* n° 215-3, p. 16.

Banque-Carrefour de la sécurité sociale prévoyait une obligation de motivation visant les traitements de données ayant permis la prise de décision.

> Ainsi, l'article 20, 1°, de ladite loi prévoyait que « les institutions de sécurité sociale sont tenues d'office [à] la communication aux bénéficiaires de la sécurité sociale [...] des données sociales à caractère personnel sur lesquelles elles se sont basées pour la détermination ou l'appréciation de leurs droits.
>
> La communication a lieu au plus tard en même temps que la notification de la décision prise au sujet du droit fondé sur les données en cause ».

En d'autres termes, les institutions de sécurité sociale étaient tenues de motiver leur décision en mentionnant, de manière bien compréhensible[1145], les données utilisées, et ce, au plus tard au moment de la notification de la décision à son destinataire. Il s'agissait d'une obligation de publicité active, conçue comme un corollaire de la collecte indirecte des données. On souhaitait, en effet, éviter que les échanges de données entre administrations diminuent la possibilité des administrés de vérifier l'exactitude des informations utilisées.

> Comme l'affirment les discussions préparatoires à l'adoption de cet article 20, « le devoir actif d'information dans le chef des institutions de sécurité sociale permet d'éviter qu'un échange de données plus intense entre les institutions, allant de pair avec une réduction importante de la collecte des informations auprès des assurés sociaux eux-mêmes, ne conduise à des possibilités moindres des bénéficiaires de vérifier l'exactitude de l'appréciation de leurs droits »[1146].

Certes, les institutions de sécurité sociale pouvaient, à l'époque, être provisoirement dispensées de respecter cette obligation[1147]. C'était toutefois à la condition d'établir une réelle impossibilité. Répondait à cette hypothèse la nécessité d'un délai pour adapter leurs outils informatiques, leur structure administrative et leur méthode de travail à l'informatisation de l'administration.

On peut raisonnablement soutenir qu'une telle dispense ne pourrait plus être obtenue aujourd'hui, la grande majorité des administrations s'étant adaptées au fonctionnement à l'e-gouvernement. Lors d'une

---

[1145] Cette exigence d'intelligibilité de la communication des données utilisées ressort des travaux préparatoires de ladite disposition (Projet de loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *Doc. Parl.,* Ch. Repr., sess. 1988-1989, n° 899/1, *Pasin.,* 1990, t. I, p. 86).

[1146] Projet de loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *Doc. Parl.,* Ch. Repr., sess. 1988-1989, n° 899/1, *Pasin.,* 1990, t. I, p. 86.

[1147] Art. 20, 1°, 3e al., de la loi du 15 janvier 1990.

demande de dispense il y a une vingtaine d'années, le Ministre des Affaires sociales a affirmé que les caisses d'allocations familiales, notamment, seraient en mesure de respecter l'obligation de communication des données à la fin de l'année 1996[1148]. Il est également amusant de constater qu'à l'époque déjà, le Ministre a mis en évidence le fait que l'adaptation des services publics à l'informatisation était d'autant plus difficile que la législation en la matière était peu claire. Ainsi a-t-il affirmé que « les différents problèmes pratiques [liés à l'informatisation de l'administration], interviennent dans un contexte juridique pour le moins mouvant, en raison des chevauchements de la loi du 15 janvier 1990 et des législations relatives à la motivation formelle des actes administratifs (loi du 29 juillet 1991), à la protection de la vie privée (loi du 8 décembre 1992) et à la publicité de l'administration (loi du 11 avril 1994). Une coordination et une harmonisation de ces législations s'impose »[1149]. Près de vingt ans plus tard, cette difficulté est toujours d'actualité…

b) L'obligation de communiquer les données remplacée par l'obligation de motiver la décision : un recul ? Bien que la solution consacrée par l'article 20 de la loi du 15 janvier 1990 soit judicieuse, l'obligation de communication des données a été remplacée par un renvoi à la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs. Cette modification discrète a fait l'objet d'une disposition enfouie parmi les 191 autres d'une loi portant des dispositions sociales de 1996[1150].

> L'article 20, §1, de la loi du 15 janvier 1990 prévoit aujourd'hui que « les articles 2 à 5 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs sont applicables aux actes administratifs unilatéraux des institutions de sécurité sociale permettant de déterminer, d'apprécier ou de modifier les droits des bénéficiaires de la sécurité sociale ou de ceux qui demandent à en bénéficier ».

En guise de justification de cette modification, il a été soutenu que la loi du 29 juillet 1991 est « plus large et offre davantage de garanties par rapport à l'obligation de l'actuel article 20 »[1151].

[1148] CPVP, avis n° 26/94 du 15 décembre 1994 relatif à un projet d'arrêté royal dispensant les caisses d'allocations familiales visées aux articles 19, 3l, 32 et 33 des lois coordonnées relatives aux allocations familiales pour travailleurs salariés, de communiquer d'office aux bénéficiaires du régime desdites lois coordonnées, les données sociales à caractère personnel sur lesquelles elles se sont fondées pour la détermination ou l'appréciation de leurs droits.

[1149] CPVP, avis n° 26/94, p. 4, n° 2.9.

[1150] Art. 67 de la loi portant des dispositions sociales du 29 avril 1996, *M.B.,* 30 avril 1993.

[1151] Projet de loi portant des dispositions sociales, *Doc. Parl.,* Ch. repr., sess. 1995-1996, n° 352/1, p. 43.

La CPVP, la section de législation du Conseil d'État, ainsi que certains parlementaires, ont contesté la véracité d'une telle justification, au motif que la loi du 29 juillet 1991 et l'obligation de communiquer les données ne poursuivaient pas le même but. Par conséquent, l'obligation de motivation formelle de la décision peut être respectée en communiquant moins de données que ne l'aurait imposé ledit article 20.

De l'avis de la CPVP, « l'obligation de motiver a pour but de permettre à l'intéressé d'apprendre pourquoi une décision a été prise à son détriment, afin qu'il puisse, par les voies de recours dont il dispose, se défendre contre cette décision [...]. Des données ne pouvant pas, selon l'administration, justifier la décision ne tombent pas sous l'obligation de motivation ». Par contre, « l'obligation imposée par l'article 20, 1er, 1°, de la loi du 15 janvier 1990, de communiquer d'office les données vise [...] à donner à la personne concernée la possibilité de vérifier l'exactitude de l'appréciation de ses droits. Pour atteindre ce but, il ne suffit pas [...] que l'institution de sécurité sociale communique seulement les données sur lesquelles elle [se base] pour justifier sa décision ; au contraire, une information correcte et complète nécessite qu'elle communique également les données qu'elle considère ne pas service de fondement à la décision prise ou, du moins, qu'elle indique [...] la voie à suivre [pour en prendre connaissance] ». Elle ajoute que « l'importance de cette dernière obligation apparaît précisément où l'institution de sécurité sociale prend une décision défavorable à la personne concernée et où elle dispose d'un plus grand nombre de données que celui qu'elle doit communiquer pour remplir l'obligation de motivation formelle ». Et de conclure en affirmant qu'« en insistant sur la motivation de la décision au lieu de l'information de la personne concernée, on en arrive [...] à un appauvrissement de l'information »[1152].

Des parlementaires se sont prononcés dans le même sens, concluant que cette modification était « de nature à réduire la protection de la vie privée »[1153].

La section de législation du Conseil d'État a soulevé la question de savoir « s'il n'aurait pas été préférable d'adapter la loi relative à la motivation », et ajoute qu' « en ce qui concerne la communication [...] de données sociales, le Conseil d'État doit constater que la loi sur la protection

[1152] CPVP, avis n° 05/96 du 5 février 1996 relatif à un projet de loi portant des dispositions sociales, chapitre IV (Banque-Carrefour de la sécurité sociale), p. 5, n° 5.

[1153] Proposition d'amendement n° 40 de M. Bacquelaine et Mme Herzet relative au projet de loi portant des dispositions sociales, *Doc. Parl.,* Ch. Repr., sess. 1995-1996, n° 352/4, p. 17 ; Projet de loi portant des dispositions sociales (art. 1er à 140 et 160 à 166), rapport fait au nom de la Commission des affaires sociales, *Doc. Parl.,* Ch. Repr., sess. 1995-1996, n° 352/11, pp. 42-43.

de la vie privée n'impose pas l'obligation d'effectuer d'office ces actes, contrairement au texte existant de l'article 20, §1er, de la loi relative à la Banque-Carrefour »[1154].

Force est donc de constater que l'obligation, pour les autorités administratives, de communiquer les données sur lesquelles se fondent leurs décisions constitue un moyen utile pour informer les personnes des éléments pertinents à la base des décisions qui les concernent. Le recul opéré par la loi du 15 janvier 1990 à cet égard doit être endigué. La loi du 29 juillet 1991 gagnerait, en effet, à être enrichie d'une telle obligation, qui s'inscrit pleinement dans le but poursuivi par le législateur de 1991, et qui, aujourd'hui, est rendue nécessaire par le déploiement de la collecte indirecte des données au sein de l'e-gouvernement.

319.- E-gouvernement et jargon technique. En s'aidant d'outils informatiques de traitement de données, l'autorité administrative pourrait être amenée à ne pouvoir justifier sa décision qu'en faisant état de calculs complexes et d'un jargon technique peu compréhensibles par le destinataire de la décision.

> À cet égard, l'e-gouvernement regorge de notions exotiques, telles qu'OASIS ou DIMONA, ou plus techniques, comme banque-carrefour, source authentique de données, plateforme d'échange d'informations, collecte indirecte, etc.

Or, selon le Conseil d'État, l'autorité administrative doit justifier sa décision de manière « claire et précise », sans « se réfugier derrière un langage technique ou chiffré difficilement compréhensible ou derrière l'assistance d'hommes de l'art »[1155].

> Dans le même sens, le Conseil d'État a déjà affirmé qu'il ne peut « que s'interroger sur la légalité d'une motivation formelle qui se réfère à un document à caractère nettement ésotérique, rédigé en un jargon anglicisant, mettant en avant des notions étrangères à tout honnête homme, telles que des 'types de courbe : III (V-SHAPE) ou V (linéar)' [...] pour se réfugier plus sûrement derrière l'utilisation du logiciel DECISION SHAPE ou l'application de la pondération PROMETHEE »[1156].

Dans la motivation de leurs décisions, les administrations doivent donc être particulièrement attentives au langage utilisé et faire œuvre de

---

[1154] SLCE, avis des 7 décembre 1995 et 8 décembre 1995 relatif à un avant-projet de loi sociale, *Doc. Parl.*, Ch. Repr., sess. 1995-1996, n° 352/1, p. 132.

[1155] C.E., 7 mars 2006, S.A. Constructions industrielles de la méditerranée, n° 155.931, p. 14.

[1156] C.E., 16 septembre 2004, *Société coopérative COMPUTER SCIENCES,* n° 134.986, p. 9.

pédagogie à l'égard du citoyen concerné, en expliquant les termes techniques utilisés. Elle pourrait également mentionner les coordonnées d'un agent auquel la personne pourrait s'adresser si des questions subsistaient.

320.- E-gouvernement et motivation par référence. Dans l'e-gouvernement, la motivation en fait d'une décision peut amener l'administration auteure de l'acte à faire référence à une donnée qui provient d'une autre administration. Il s'agit alors d'une motivation par référence.

a) Des exemples. C'est le cas, par exemple, lorsqu'une administration communique à une autre administration, auteure de l'acte, une information à partir de laquelle cette dernière décide de sanctionner la personne concernée. La décision de sanction se référant à l'information qui a été transférée d'une administration à l'autre est motivée par référence.

> Le Tribunal du travail de Bruxelles a connu d'une telle hypothèse, qui a donné lieu à un jugement du 19 janvier 2009. Les faits sont les suivants : durant deux ans, l'ONEm paie des allocations de garanties de revenus à Monsieur S. Par la suite, l'INASTI communique à l'ONEm l'information selon laquelle, suite à une enquête de leurs services, il est établi que Monsieur S. a perçu des revenus d'indépendants durant ces deux mêmes années. Sur la base de cette information émanant de l'INASTI, l'ONEm décide de réclamer à Monsieur S. le remboursement des allocations de garanties de revenu. Monsieur S. conteste la décision de l'ONEm devant le Tribunal du travail de Bruxelles.
>
> Dans son jugement, le Tribunal du travail affirme que « la décision contestée a utilisé la technique de la motivation par référence puisqu'elle se fonde sur la décision [...] de l'INASTI »[1157].

Une décision est également motivée par référence lorsqu'elle se réfère à la mention « oui-non ». On a préalablement souligné l'utilisation de cette méthode dans l'e-gouvernement qui consiste à ne communiquer à l'auteur de l'acte que la seule donnée selon laquelle, oui ou non, la personne concernée répond aux conditions de revenus requises pour obtenir une allocation, par exemple[1158].

b) Des difficultés. La motivation par référence à une donnée provenant d'une autre administration génère des difficultés.

En effet, la donnée à laquelle il est fait référence peut être erronée, auquel cas, la motivation de la décision administrative doit être considérée comme inadéquate.

[1157] Trib. Trav. Bruxelles, 19 janvier 2009, R.G. n° 69381/98.

[1158] Dans le premier titre de la recherche, on a souligné l'intérêt de cette méthode pour garantir la proportionnalité des données. Voy. *supra*, n° 154.-

> Dans le cas soumis au Tribunal du travail de Bruxelles, précédemment exposé, l'INASTI considère que Monsieur S. a perçu des revenus en tant qu'indépendant, alors qu'il s'agissait des allocations de garantie de revenus versées par l'ONEm. Le Tribunal décide qu' « une décision rendue par référence à une décision administrative contenant une confusion à ce point importante ne peut être considérée comme revêtue d'une motivation adéquate ».

La motivation qui se réfère à une donnée peut également être insuffisante, et dès lors, inadéquate, en ce qu'elle ne permet pas à la personne concernée de comprendre pleinement le raisonnement qui sous-tend la décision s'imposant à elle. C'est un risque particulièrement présent dans le cas de l'utilisation de la mention « oui-non ».

> Le cas suivant permet d'illustrer cette problématique. Il a été porté devant le **Médiateur fédéral**, qui le décrit en ces termes : « Madame Hermans introduit à temps sa demande de réduction énergie pour 2008. Après plus de six mois, elle reçoit une réponse négative. Dans une lettre standard, l'administration lui signale qu'elle n'a pas droit à la réduction forfaitaire d'énergie parce qu'après consultation des données auprès du SPF Finances, il est apparu qu'en 2006, le revenu annuel net imposable de son ménage dépasse le plafond de 23 282 euros qui permet de prétendre à la prime. L'administration ne précise pas le montant du revenu pris en considération [...].
>
> La motivation de la décision est cependant loin d'être claire : dans sa lettre, l'administration reprend le revenu imposable globalement et le revenu imposable séparément et arrive après addition à un total de 17 157,74 euros. Elle termine sa lettre par la conclusion pour le moins étonnante qu'étant donné que la somme susmentionnée est supérieure à 23 282,00 euros, Madame Hermans n'a pas droit à la réduction énergie pour 2008.
>
> À la demande du Médiateur fédéral, le dossier est réexaminé. [...] [Il s'avère finalement] que la décision de refus est justifiée, mais que la motivation est nettement insuffisante »[1159].
>
> Comme l'affirme le Médiateur fédéral, cette insuffisance de motivation s'explique par le fait que le SPF Economie, chargé de décider de l'octroi de l'allocation, ne communique pas au demandeur les éléments concrets sur la base desquels un refus a été décidé. Il n'est d'ailleurs pas en mesure de le faire étant donné que le SPF Economie ne reçoit du SPF Finances qu'une réponse binaire « oui-non », indiquant si oui, ou non, la personne dépasse le plafond de revenus au-dessus duquel l'allocation ne peut être octroyée[1160].

[1159] Rapport annuel du Médiateur fédéral, 2009, disponible sur le site http://www.federaalombudsman.be/sites/1070.fedimbo.belgium.be/files/09_Francais.pdf, pp. 84-85.

[1160] *Ibid.,* p. 84.

> On peut raisonnablement penser que le **Conseil d'État** estimerait également que pareille motivation est inadéquate. En effet, on peut comparer ces décisions à celles qui mentionnent, sans autre précision, que « l'intéressé ne se trouve pas dans une situation proche de l'état de besoin ». Celles-ci sont censurées par le Conseil d'État, qui juge une telle motivation stéréotypée. À propos d'une décision motivée comme suit : « [...] qu'on ne peut déduire des données relatives aux revenus de l'intéressé durant les années 2004 et 2005, que l'intéressé se trouve actuellement dans un état de besoin ou dans une situation voisine de l'état de besoin », le Conseil d'État soutient que « les décisions de la Commission refusant en tout ou en partie la dispense, doivent, pour être formellement et adéquatement motivées, permettre de comprendre quels éléments concrets ont été pris en considération pour déterminer si le demandeur se trouve ou non dans un état de besoin ou dans une situation proche de l'état de besoin ; que la décision attaquée ne comporte qu'une motivation stéréotypée, qui ne permet pas de comprendre quels sont les revenus et les charges qui ont été prises en considération[1161] par la commission pour refuser la dispense ; que le moyen pris de la violation des article 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs est fondé »[1162]

c) Des solutions à envisager. Pour que la motivation par référence soit adéquate, le citoyen doit connaître et comprendre la donnée ou la décision à laquelle l'auteur de l'acte se réfère, et ce, au plus tard au moment de la notification de l'acte juridique[1163]. Pour ce faire, l'auteur de l'acte peut annexer à sa décision un document qui livre des explications sur la donnée ou la décision à laquelle il se réfère[1164].

En outre, l'obligation de motivation formelle qui s'impose à chaque administration doit être soutenue, dans l'e-gouvernement, par la mise en place d'outils technologiques qui facilitent les démarches du citoyen désireux de comprendre d'où viennent les données utilisées, si elles sont exactes, si elles pouvaient légalement être transférées, etc. Il importe, en effet, que la personne concernée ait d'emblée une vision claire des données utilisées, de leur origine et des autorisations de comités sectoriels attestant de la légalité des échanges réalisés. Le cas échéant, elle doit également pouvoir prendre contact avec l'administration responsable de la source authentique pour

---

[1161] C'est nous qui soulignons.

[1162] C.E., arrêt *Holbrecht,* n° 193.423, du 19 mai 2009. Pour d'autres références à des arrêts portant sur une question similaire, voy. X. Delgrange et B. Lombaert, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : questions d'actualité », *op. cit.,* p. 48, note 214.

[1163] Voy., not., C.E., arrêt *K.C.L.,* n° 213.676, n° 213.676, du 6 juin 2011.

[1164] Voy. not. C.E., arrêt *Mahaux,* n° 189.817, du 27 janvier 2009 ; arrêt *ASBL Academy of security,* n° 114.070, du 20 décembre 2002.

vérifier l'exactitude de la donnée utilisée et la corriger si nécessaire. Si la donnée est une mention « oui-non », elle pourrait également obtenir de l'administration émettrice de cette information les détails du calcul ayant abouti à la mention « oui » ou « non ». Des solutions pour parvenir à ces objectifs sont proposées dans le troisième chapitre.

*

Conclusions

321.- La transparence : une exigence fondamentale dans un État de droit. La première partie de ce chapitre a souligné l'importance de l'exigence de transparence dans un État de droit. Le temps est révolu d'une administration secrète et distante, se réfugiant derrière l'opacité de son action. Des puits de lumière sont à présent creusés dans cette forteresse, qui doivent permettre au citoyen de savoir et de comprendre ce qu'il se passe derrière les murs de l'administration. Fort de cette prise de conscience, il peut ainsi participer en pleine connaissance de cause au processus démocratique, dans le prolongement de la liberté d'expression et d'information consacrée à l'article 10 de la Convention européenne des droits de l'homme. Il est également en mesure de contrôler l'action administrative, et d'établir une relation de confiance avec les autorités publiques, qui se voient ainsi légitimées dans leurs choix.

322.- Les forces du régime de la transparence administrative. Le constituant et le législateur ont bien compris cet impératif démocratique, et se sont attelés à baliser les voies d'accès vers l'administration, faisant de la transparence la règle et du secret, l'exception. Le citoyen s'en trouve nanti de droits non négligeables.

La publicité de l'administration est consacrée par un droit fondamental – l'article 32 de la Constitution – et organisée par la loi du 11 avril 1994 relative à la publicité de l'administration, ainsi que plusieurs normes décrétales ayant le même objet. Ces normes confèrent au citoyen le droit d'accéder aux documents détenus par les autorités administratives. La confidentialité ne peut lui être opposée qu'en invoquant certaines exceptions, à interpréter strictement. La voie de la publicité active est également ouverte par les législateurs du pays. Par ailleurs, la transparence suppose aussi que les administrés comprennent les décisions qui les visent. La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs s'inscrit dans cette perspective.

Grâce à cet arsenal normatif, le citoyen peut prendre connaissance des documents qui lui permettent de comprendre l'action administrative dans son ensemble.

323.- Les limites du régime de la transparence administrative. Il n'en demeure pas moins que le régime de la transparence administrative a une vingtaine d'années et est imprégné d'une vision « papier » de l'administration. Dès lors, cette réglementation traditionnelle peine à s'adapter de manière satisfaisante aux évolutions technologiques contemporaines.

La *publicité de l'administration* est ébranlée par l'e-gouvernement, comme l'a montré la deuxième section de ce chapitre. Les concepts utilisés dans cette législation doivent être actualisés face à la disparition progressive du papier, qui est remplacé par des courriers électroniques et des bases de données à la structure particulière et complexe. Plus encore, la logique du droit d'accès, qui sous-tend la publicité de l'administration, doit être repensée. En effet, une telle conception de la transparence exige du citoyen qu'il identifie et sollicite lui-même les documents recherchés. Ces tâches deviennent de plus en plus complexes, au fur et à mesure que des réseaux sectoriels sont créés, que les informations sont éparpillées entre diverses sources authentiques de données, et que sont utilisées des méthodes de travail jusqu'alors inédites, fondées sur des outils complexes, générant des documents d'un genre nouveau.

Face à cette révolution, comment un citoyen peut-il raisonnablement se douter de l'existence de certains documents et des conséquences de certains outils ? Comment peut-il préciser suffisamment ses demandes d'accès alors que la matière est si complexe que même les agents de l'administration n'ont pas une vue précise et complète des nouveautés en vigueur ?

C'est pourquoi, la vieille logique du droit d'accès doit être dépassée au profit d'un déploiement plus franc de la publicité active, comme cela a déjà été fait pour la publicité des informations environnementales. L'administration est aujourd'hui techniquement capable de diffuser, en ligne, tous les documents dont elle dispose. Il est de son devoir de le faire, pour adapter la publicité de son action aux méthodes nouvelles qu'elle emploie.

Finalement, comme en témoigne la troisième partie de ce chapitre, la loi du 29 juillet 1991 sur la *motivation formelle des actes administratifs,* elle aussi, n'offre plus que d'insuffisantes réponses au citoyen désireux de comprendre pourquoi telle décision a été prise à son égard. De plus en plus souvent, l'institution ne peut se prononcer sur le cas d'un administré qu'après un échange de données provenant d'une autre autorité. Telle est la conséquence du principe de collecte unique des données. L'administration, auteur de la décision, n'a pas vérifié la qualité des données, ni la légalité de l'échange effectué. Bien

souvent, elle n'était même pas en mesure de le faire, ne connaissant pas elle-même l'origine des données qui lui ont été fournies.

Le citoyen est-il en mesure d'en savoir plus ? Actuellement, la négative prévaut. Les transferts de données ne semblent constituer que des mesures préparatoires à la décision finale, qui ne doivent pas être motivées. Le destinataire de la décision doit donc se contenter de la décision finale, sans que soient fournis les motifs relatifs aux données utilisées. On comprend que le citoyen s'en ressente frustré, en particulier s'il se voit contraint de se soumettre à une décision négative.

Face à ces bouleversements, il s'impose d'enrichir la transparence administrative, afin d'offrir aux citoyens davantage de moyens pour comprendre finement l'e-gouvernement. À cet égard, l'étude de la transparence des traitements de données à caractère personnel, consacrée par le régime de protection des données à caractère personnel, présente un grand intérêt. Le chapitre suivant y est consacré.

*

CHAPITRE II.
L'e-gouvernement et la transparence des traitements de données à caractère personnel

Introduction

Comme l'a souligné le premier titre de la recherche, la transparence des traitements de données à caractère personnel doit, avant tout, être assurée par le législateur. En effet, l'article 22 de la Constitution impose au pouvoir législatif d'adopter des normes claires et précises, déterminant les éléments cardinaux des traitements de données mis en place au sein de l'administration. Ainsi, comme l'affirme la CPVP, « la qualité de la base légale doit être prioritaire »[1165].

Il n'en demeure pas moins que les normes légales sont générales et abstraites. Quand bien même elles seraient très bien rédigées – ce qui, rappelons-le, n'est pas nécessairement le cas aujourd'hui – le citoyen n'y trouvera pas nécessairement de réponse aux questions qu'il se pose sur l'utilisation de ses propres données.

C'est pourquoi, les normes relatives à la protection des données à caractère personnel offrent plusieurs voies pour assurer la transparence des traitements de données à caractère personnel.

*

Section 1. La notion de transparence des traitements de données à caractère personnel

324.- Définition. La transparence des traitements de données à caractère personnel vise l'ensemble des règles qui organisent le droit des

[1165] CPVP, avis n° 23/2008 du 11 juin 2008 relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules, p. 32.

personnes dont les données sont traitées, d'avoir connaissance de ces traitements et de leurs modalités.

Ces règles trouvent leur raison d'être dans la nécessité d'assurer l'autodétermination informationnelle des personnes concernées. Plusieurs obligations tendent à atteindre cet objectif.

I. La raison d'être de la transparence des traitements de données à caractère personnel

325.- L'article 8 de la Convention européenne des droits de l'homme. Le souci de transparence accompagnait déjà les premières discussions relatives à l'encadrement normatif des traitements de données à caractère personnel en vue de protéger la vie privée des personnes concernées.

> Ainsi, la Résolution (74) 29 du Conseil de l'Europe relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électronique dans le secteur public, adoptée le 20 septembre 1974, affirme déjà que « chaque personne a le droit de connaître les informations enregistrées sur elle. Toute exception à ce principe ou limitation à l'exercice de ce droit doit être strictement réglementée ».
>
> Le Rapport explicatif de la Convention n° 108 souligne que « toutes les lois nationales reconnaissent le principe de publicité, c'est-à-dire que l'existence de fichiers automatisés de données soit portée à la connaissance du public »[1166].
>
> Les discussions préalables à l'adoption de la loi du 8 décembre 1992 présentent la transparence comme « une des caractéristiques principales [du] projet de loi »[1167].

L'attention portée à la transparence des traitements de données à caractère personnel s'explique par la nécessité d'assurer l'effectivité du droit à l'autodétermination informationnelle[1168], en vertu duquel chacun a le droit de garder la maîtrise sur ses propres données. L'effectivité du droit à l'autodétermination informationnelle est directement liée à la transparence des traitements de données à caractère personnel. En effet,

[1166] Rapport explicatif de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, point 6.

[1167] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la Commission de la Justice par Mme Merckx-Van Goey, *Doc. Parl.,* Ch. Repr., sess. 1991-1992, n° 413/12, p. 10.

[1168] Voy. *supra*, n°s 61.- et s.

rappelons[1169] que « 'maîtriser' ne signifie pas nécessairement choisir et déterminer ce qui est communiqué à autrui. Il s'agit surtout d'avoir accès aux données conservées et/ou utilisées par d'autres et d'avoir connaissance du sort réservé à ces données »[1170].

Concrètement, la transparence des traitements de données à caractère personnel répond à ce droit fondamental car elle permet au citoyen d'avoir *conscience* du fait que ses données sont collectées et traitées. Ce dernier peut également identifier les autorités impliquées dans ces processus ainsi que les raisons qui justifient les traitements[1171].

En outre, consciente que ses données sont traitées, et bénéficiant des informations à ce sujet, la personne concernée est en mesure de *vérifier l'exactitude* des données utilisées[1172]. Cela bénéficie tant au citoyen qu'à l'administration, qui ont tous intérêt à ce que des erreurs n'affectent pas les données utilisées. Il en va d'autant plus ainsi que les informations seront échangées et réutilisées de nombreuses fois.

Enfin, la transparence permet au citoyen de *contrôler l'usage* de ses données personnelles, en vérifiant qui a accédé à ses informations et dans quel but[1173]. Tout administré peut ainsi jouer « un rôle d'avertisseur puisqu'il est le mieux placé pour détecter des consultations 'anormales' pouvant donner lieu à des sanctions »[1174]. En outre, l'existence d'une possibilité de contrôle incite les administrations à traiter les données en leur possession conformément à la loi. C'est d'ailleurs ce que rappelle la CPVP en soutenant que « le fait de savoir que le citoyen, qui est le mieux placé pour détecter quand ses données ont été consultées à tort, dispose d'un tel droit de consultation ne peut qu'influencer positivement l'utilisation correcte [des données] »[1175].

Le résultat de la transparence des traitements de données à caractère personnel rejoint celui de la transparence administrative étudiée dans le

---

[1169] Voy. *supra,* n° 64.-

[1170] C. DE TERWANGNE, « Le rapport de la vie privée à l'information », *in Droit des technologies de l'information. Regards prospectifs* (dir. E. MONTERO), Bruxelles, Bruylant, 1999, p. 138.

[1171] C. DE TERWANGNE, « Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles : regards croisé sur deux voies d'accès à l'information », *Transparence et droit à l'information,* Liège, Formation permanente CUP, 2003, p. 90.

[1172] Projet de loi relatif à la protection de certains aspects de la vie privée, *op. cit.,* n° 778/1, p. 14.

[1173] *Idem.*

[1174] CPVP, avis n° 12/2009 du 29 avril 2009 relatif à une demande d'avis émanant du SPF Intérieur concernant un certain nombre de questions qui se sont posées dans le cadre de la délibération RN n° 19/2008, p. 6.

[1175] CPVP, recommandation n° 03/2009 du 1er juillet concernant les intégrateurs dans le secteur public, p. 10.

premier chapitre, en ce qu'elle participe également à l'amélioration de la démocratie. En effet, la transparence des traitements de données à caractère personnel tend à équilibrer le pouvoir de l'État et des citoyens en permettant à ces derniers d'intervenir, en pleine connaissance de cause, dans les débats relatifs aux questions soulevées par l'e-gouvernement. Ce faisant, on instaure un « contrôle démocratique, exercé par les citoyens eux-mêmes »[1176]. La transparence des traitements de données à caractère personnel favorise également la confiance des citoyens en leurs institutions, nécessaire à l'accomplissement des fonctions étatiques.

II. Le contenu de la transparence des traitements de données à caractère personnel

326.- Un droit de savoir. Les règles relatives à la transparence des traitements de données à caractère personnel garantissent aux citoyens un droit de savoir quelles données sont collectées, et à quels traitements elles sont soumises[1177].

Certains mécanismes se raccrochent à ce qu'on appelle traditionnellement la *publicité passive* de l'administration, en ce sens, rappelons-le, que la divulgation des informations est tributaire d'une initiative des personnes intéressées. Il s'agit du droit d'accès aux données à caractère personnel[1178], qui s'accompagne d'un droit de rectification des données erronées et d'un droit d'opposition[1179].

D'autres obligations s'imposent aux administrations lorsqu'elles traitent des données, qui s'apparentent à de la *publicité active* puisqu'elles contraignent les autorités à divulguer les informations sans attendre une démarche du citoyen. Il s'agit de l'obligation d'informer les personnes

[1176] Projet de loi relatif à la protection de certains aspects de la vie privée, *Doc. Parl.*, Ch. Repr., sess. 1983-1984, n° 778/1, p. 14.

[1177] Comme l'affirment les travaux préparatoires de la loi du 8 décembre 1992, « ce droit de savoir, ce droit à l'information est inséré dans le projet à plusieurs endroits et est garanti à l'intéressé » (Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la Commission de la Justice par Mme Merckx-Van Goey, *Doc. Parl., op. cit.*, n° 413/12, p. 10.

[1178] Convention n° 108, art. 8, b) ; Directive 95/46, art. 12, a) ; Loi du 8 décembre 1992, art. 10.

[1179] Convention n° 108, art. 8, c) ; Directive 95/46, art. 12, b) ; Loi du 8 décembre 1992, art. 12.

dont les données sont traitées[1180], de l'obligation de déclaration de tels traitements et de la tenue d'un registre public[1181].

327.- L'absence d'une obligation de motivation. À l'heure actuelle, aucune des normes relatives aux traitements de données ne prévoit d'obligation de motivation qui imposerait aux administrations de communiquer aux administrés les données utilisées dans le cadre des décisions prises. Nous y reviendrons dans le troisième chapitre.

Section 2. La publicité passive des traitements de données à caractère personnel

328.- L'article 10, §1, de la loi du 8 décembre 1992. L'article 10, §1, de la loi du 8 décembre 1992, organise le droit d'accès du citoyen à ses données à caractère personnel.

> Il dispose que « la personne concernée qui apporte la preuve de son identité a le droit d'obtenir du responsable du traitement :
>
> a) la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ;
>
> b) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données ;

[1180] En ce sens, l'art. 8, a), de la Convention n° 108 dispose que « Toute personne doit pouvoir connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier » (néanmoins, dans leur Rapport sur les lacunes de la Convention n° 108, Cécile de Terwangne et Jean-Philippe Moiny soutiennent que « la formulation de ce principe n'est assurément pas suffisamment indicative d'un devoir de transparence spontané », et proposent de le mentionner plus clairement) (voy. C. DE TERWANGNE et J.-P. MOINY, *Rapport sur les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (partie II) pour le Bureau du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, novembre 2010, p. 29, note 78). La section IV de la directive 95/46/ CE qui s'intitule « Information de la personne concernée » consacre plusieurs dispositions à ce sujet. La loi du 8 décembre 1992 impose l'obligation d'information en son art. 9.

[1181] Directive 95/46/CE, section IX, art. 18 à 21 ; Loi du 8 décembre 1992, art. 18 à 20.

c) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, dans le cas des décisions automatisées visées à l'article 12*bis* ;

d) un avertissement de la faculté d'exercer les recours prévus aux articles 12 et 14 et, éventuellement, de consulter le registre public prévu à l'article 18 ».

À la lecture de la loi du 8 décembre 1992, le droit d'accès paraît idéalement organisé. Il doit permettre à chacun de dresser le schéma de l'ensemble des traitements de données qui le concernent. Néanmoins, en pratique, l'exercice du droit d'accès à l'égard de l'administration se révèle semé d'embûches et gagnerait à être simplifié.

I. La procédure d'accès aux données à caractère personnel

329.- Considérations générales. Après avoir expliqué en quoi consiste le droit d'accès organisé par la loi du 8 décembre 1992, on pointe les limitations du droit d'accès, qui affectent la transparence des traitements de données à caractère personnel.

A. Le droit d'accès

330.- Des conditions à respecter. L'exercice du droit d'accès suppose que la personne concernée introduise une demande respectant certaines prescriptions de forme et de contenu.

§1. La demande d'accès

331.- La forme de la demande. L'article 32 de l'arrêté royal du 13 février 2001[1182] organise la forme de la demande d'accès.

La demande doit être datée et signée. Il y a lieu de l'adresser au responsable du traitement ou au sous-traitant qui communique la demande au responsable[1183]. L'identité du demandeur doit être justifiée, si bien que la demande doit être accompagnée d'une copie de la carte d'identité.

[1182] Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001.

[1183] Sur la désignation du responsable du traitement dans l'administration, voy. *supra*, n°s 75.- et s.

La demande est remise sur place ou envoyée par la poste ou « par tout moyen de télécommunication ». Cela signifie que la demande peut être introduite par courriel, à la condition de faire figurer une signature électronique afin de prouver l'identité de son auteur, comme le requiert l'article 10, §1, alinéa 1, de la loi du 8 décembre 1992.

332.- La formulation de la demande. La demande d'accès sur la base de la loi du 8 décembre 1992 est plus aisée à formuler que celle fondée sur la loi du 11 avril 1994 précédemment analysée.

En effet, le demandeur ne doit pas cibler un document ni même une matière particulière. Il suffit pour lui de faire savoir à l'administration qu'il souhaite accéder à ses données à caractère personnel, à charge, pour l'institution, de retrouver ces informations dans ses fichiers. Il s'agit donc là d'un accès par le contenu, et non par le contenant.

333.- L'objet de la demande. Le demandeur peut demander au responsable de traitement plusieurs informations concernant ses données à caractère personnel, en vertu de l'article 10, §1, de la loi du 8 décembre 1992.

> Signalons que, pour faciliter la tâche du citoyen, la CPVP met à sa disposition une lettre type comprenant notamment la liste des types d'informations qui peuvent être demandées au responsable de traitement, à charge pour le demandeur d'accès de cocher la ou les types d'informations qu'il réclame[1184].

a) Les données. À la demande de la personne concernée, le responsable du traitement est tenu de *confirmer* ou non qu'il détient des données.

Dans l'affirmative, il doit indiquer le *type* de données concernées (nom, prénom, etc.).

Une copie des *données exactes* peut également être exigée. Toutefois, le responsable du traitement détermine lui-même la forme de la copie. Il ne doit pas nécessairement donner un extrait de la base de données dans laquelle la personne concernée est enregistrée, et peut se contenter de fournir les informations par téléphone, par exemple[1185].

b) Les indications relatives à certains aspects du traitement des données. Le responsable du traitement doit également fournir des indications

[1184] Cette lettre type est disponible à l'adresse http://www.privacycommission.be/fr/exercice-droit-acces/vos-possibilites.

[1185] Site internet de la CPVP (www.privacycommission.be), rubrique En pratique : vie privée – principes de base.

relatives à la collecte, à l'enregistrement et à l'utilisation future des données.

Ainsi doit-il indiquer la *finalité* en vue de laquelle il détient les données. Rappelons que, s'agissant d'une administration, cette finalité doit faire partie des missions légalement attribuées à celles-ci.

En outre, il doit fournir des explications sur l'*origine* des données. Ce faisant, la personne concernée est en mesure de savoir d'où proviennent les informations. Elle peut ainsi retracer le parcours suivi par les données, et contester éventuellement les communications effectuées. Ce pourrait être le cas, par exemple, si la finalité de la communication des données n'est pas compatible avec celle de leur collecte[1186].

Enfin, la personne concernée a le droit de connaître les *destinataires* des données, c'est-à-dire les catégories de personnes auxquelles les données ont été communiquées ou le seront ultérieurement.

c) La logique qui sous-tend les décisions automatisées. Une personne soumise à une décision automatisée visée à l'article 12*bis* de la loi du 8 décembre 1992 a le droit d'accéder aux éléments lui permettant de comprendre la logique qui sous-tend celle-ci.

En vertu de l'article 12*bis* de la loi du 8 décembre 1992, une décision automatisée est une « décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative » qui est prise « sur le seul fondement d'un traitement automatisé de données destiné à évaluer sa personnalité ». Les décisions de ce type sont autorisées pour autant qu'elles soient fondées sur « une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance ».

Comme on l'a dit à plusieurs reprises, dans l'e-gouvernement, des personnes sont considérées comme des possibles fraudeurs et, dès lors, soumises à des contrôles particuliers, suite à l'utilisation d'outils de profilage tels que l'entrepôt de données OASIS qui les identifie de manière automatisée. Ces personnes ont-elles le droit d'accéder aux critères abstrait de sélection qui représentent la logique sous-tendant la décision de les contrôler ?

> En guise d'illustration, on évoque à nouveau[1187] le cas du dentiste régulièrement contrôlé par l'INAMI. Peut-il invoquer le droit d'accès organisé par la loi du 8 décembre 1992 pour connaître les critères qui amènent l'administration à considérer si souvent son dossier comme suspect ?

[1186] C. DE TERWANGNE, « Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles : regards croisé sur deux voies d'accès à l'information », *op. cit.,* p. 106.

[1187] Voy. *supra,* n° 281.-

La réponse n'est pas évidente. En effet, l'article 12*bis* soulève nombre de questions d'interprétation qui rendent incertaine son application au cas spécifique du profilage. Ainsi, qu'est-ce qu'une décision « affectant la personne de manière significative » ? Qu'est-ce qu'un traitement de données « destiné à évaluer sa personnalité » ? Par ailleurs, peut-on considérer que le contrôle d'un individu suite à l'utilisation d'OASIS est effectué « sur le seul fondement d'un traitement de données automatisé », dans la mesure où l'utilisation d'OASIS ne fait que guider l'administration dans le choix des personnes à contrôler, mais ne dispense pas les agents d'effectuer une inspection traditionnelle sur le terrain ?[1188]

Les opérations de profilage à partir de données à caractère personnel sont appelées à se développer et se multiplier au sein de l'administration, compte tenu du gain qu'elles offrent en termes d'efficacité pour cibler les fraudeurs avec une probabilité forte que cela s'avère exact sur le terrain. Pour le citoyen, de tels traitements de données sont particulièrement obscurs. Ils sont si complexes qu'il n'en comprend pas la logique et en ignore bien souvent l'existence. Comment, dans ce contexte, garantir aux individus la maîtrise de leur image informationnelle, comme le prévoit le droit à la protection de la vie privée ?

Une solution serait d'étendre le droit d'accès des personnes concernées au-delà de ce que prévoient actuellement les articles 10 et 12*bis* de la loi du 8 décembre 1992, en ne le conditionnant pas à l'existence d'une « décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ». En effet, « le simple fait d'avoir été l'objet d'un profilage automatisé destiné à évaluer certains aspects de sa personnalité doit ouvrir à l'individu le droit à en être informé, à pouvoir accéder à la logique du profilage et à s'opposer, au moins dans certains cas à un traitement automatisé censé pouvoir évaluer certains aspects de sa personnalité ».[1189]

[1188] Sur les difficultés générées par l'art. 15 de la directive 95/46/CE (que transpose l'art. 12*bis* de la loi du 8 décembre 1992) et un commentaire de cette disposition, voy. L. Bygrave, « Minding the Machine : Art. 15 of the EC Data Protection Directive and Automated Profiling », *Computer Law & Security Report,* 2001, vol. 17, pp. 17-24, disponible en ligne sur le site http://www.austlii.edu.au/au/journals/PLPR/2000/40.html ; J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, *L'application de la Convention 108 au mécanisme de profilage. Eléments de réflexion destinés au travail futur du Comité consultatif. Rapport pour le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,* 11 janvier 2008, pp. 14 et 15.

[1189] Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *L'application de la Convention 108 au mécanisme de profilage. Eléments de réflexion destinés au travail futur du Comité consul-*

C'est en ce sens que se prononce la CPVP, à propos des outils de profilage utilisés en matière fiscale. Elle soutient que l'accès à la logique qui sous-tend une décision automatisée ne doit pas se limiter aux décisions finales. « Toute décision automatisée ayant un effet sur la situation fiscale d'un contribuable doit être portée à la connaissance du contribuable en même temps que les données qui ont été collectées à cet effet et leur origine »[1190].

> Ce faisant, le dentiste dont le cas a été précédemment évoqué pourrait exiger de connaître les critères abstraits utilisés par l'INAMI dans sa sélection des possibles fraudeurs, dans la mesure où cette sélection est automatisée et s'effectue à partir des données à caractère personnel détenue par cette institution.

§2. La réponse de l'administration

334.- La communication des informations. L'administration sollicitée doit fournir au demandeur l'ensemble des informations demandées, sous réserve des exceptions organisées au bénéfice de certaines autorités publiques, qui sont examinées ci-après.

La réponse doit intervenir endéans les 45 jours de la réception de la demande[1191].

335.- L'indication des recours. Comme c'est le cas dans la loi du 11 avril 1994 relative à la publicité de l'administration, la réponse de l'administration contenant la communication des informations susvisées doit être assortie de la mention des différents recours à disposition de la personne concernée[1192]. Il s'agit d'un recours en rectification auprès du responsable du traitement, pour obtenir les corrections des éventuelles données erronées[1193] et d'un recours en opposition, également auprès du

---

tatif. Rapport de J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, 11 janvier 2008, pp. 14 et 15 disponible sur le site http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profilage_2008_fr.pdf

[1190] CPVP, avis n° 01/2007 du 17 janvier 2007 concernant un avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances, pp. 15 et 16.

[1191] Art. 10, §1, 3e al., de la loi du 8 décembre 1992.

[1192] Ces recours sont détaillés dans le troisième titre de la recherche. Voy. *infra,* nos 469.- et s.

[1193] L'art. 12, §1er, al. 1, de la loi du 8 décembre 1992, dispose que « toute personne a le droit d'obtenir sans frais la rectification de toute donnée à caractère personnel inexacte qui la concerne ».

responsable du traitement, afin d'empêcher le traitement des données[1194]. Il s'agit, par ailleurs, d'un recours judiciaire devant le président du tribunal de première instance siégeant comme en référé, pour contraindre le responsable de traitement de communiquer les données demandées, de les rectifier ou de cesser le traitement de celles-ci[1195].

B. Les limitations du droit d'accès

336.- Des dispenses en faveur des autorités publiques. L'article 3, §§4, 5, 6, de la loi du 8 décembre 1992 prévoit d'importantes limitations au droit d'accès, applicables au secteur public.

Ainsi, plusieurs autorités publiques ne sont pas soumises aux obligations de transparence qui viennent d'être décrites. Il s'agit notamment des autorités publiques pour les traitements de données effectués en vue de l'exercice de leurs missions de police judiciaire[1196] et des autorités publiques pour les traitements effectués en vue de leurs missions de police administrative[1197]. La sûreté de l'État, le service général du renseignement et de la sécurité des forces armées, le Comité permanent de contrôle des services de renseignements et son service d'enquête font également partie des institutions bénéficiant de cette exception, pour les traitements de données nécessaires à l'exercice de leurs missions[1198].

337.- Un déséquilibre entre l'État et le citoyen.

a) L'accès indirect aux données : un accès fictif. Officiellement, dans les hypothèses visées à l'article 3, §§ 4, 5 et 6, de la loi du 8 décembre 1992, les personnes concernées bénéficient d'un accès indirect aux traitements de leurs données, c'est-à-dire qu'elles peuvent en principe exercer leur droit d'accès par l'intermédiaire de la CPVP.

> En effet, l'article 13, alinéa 1er, de la loi du 8 décembre 1992 affirme que « pour exercer [son droit d'accès] à l'égard des traitements de données à

[1194] L'art. 12, §1er, al. 2, de la loi du 8 décembre 1992 dispose que « toute personne a le droit de s'opposer, pour des raisons sérieuses et légitimes tenant à une situation particulière, à ce que les données la concernant fassent l'objet d'un traitement ». Néanmoins, il est fait exceptions à ce droit lorsque la licéité du traitement est basée sur les motifs visés à l'art. 5, *b* et *c*. Cette exception sera analysée plus loin.

[1195] Ce recours est prévu à l'art. 14 de la loi du 8 décembre 1992.

[1196] Art. 3, §5, 1° de la loi du 8 décembre 1992.

[1197] Dans cette hypothèse, les autorités publiques doivent avoir été désignées par un arrêté royal délibéré en Conseil des ministres, après avis de la CPVP. Voy. l'art. 3, §5, 3°, de la loi du 8 décembre 1992.

[1198] Art. 3, §4, de la loi du 8 décembre 1992.

> caractère personnel visés à l'article 3, §§ 4, 5 et 6 », « toute personne justifiant de son identité a le droit de s'adresser sans frais à la Commission de la protection de la vie privée ».

À la lecture de ces lignes, la personne concernée peut raisonnablement s'attendre à recevoir la communication des informations demandées, une fois que la CPVP a ôté du document communiqué les données confidentielles.

Néanmoins, en réalité, il n'en est rien. L'article 13 de la loi du 8 décembre 1992 limite considérablement l'ampleur de la réponse qui doit être donnée au demandeur d'accès. Concrètement, aucune donnée ne lui est communiquée[1199].

Ainsi, l'article 13, alinéa 2, prévoit que « la Commission de la protection de la vie privée communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires ».

b) Des exceptions larges. De telles dispenses en faveur des autorités publiques sont larges, si bien que la loi du 8 décembre 1992 semble affaiblir de manière disproportionnée la possibilité du citoyen de contrôler l'usage qui est fait de ses données. Un déséquilibre est ainsi créé entre les intérêts de sécurité et de défense de l'État et ceux des citoyens dont les données sont traitées[1200].

En ce sens, la section de législation du Conseil d'État s'est par exemple opposée à l'utilisation des termes « police administrative »[1201] comme motif justifiant que les traitements de données effectués dans ce but ne soient pas soumis aux obligations de transparence prévues à l'article 10 de la loi du 8 décembre 1992. Ainsi affirme-t-elle que « selon l'acception usuelle des mots 'police administrative', la disposition aurait pour résultat de soustraire de nombreux fichiers publics au droit d'accès, ce qui serait

---

[1199] Dans le même sens, voy. C. DE TERWANGNE, « Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles : regards croisés sur deux voies d'accès à l'information », *op. cit.,* p. 107.

[1200] En ce sens, B. HAVELANGE et Y. POULLET, « Secret d'État et vie privée : ou comment concilier l'inconciliable ? » in *Droit des technologies de l'information : regards prospectifs* (dir. E. MONTERO), Bruxelles, Bruylant, 1999, p. 234.

[1201] Signalons que la notion de police administrative peut être définie comme « l'ensemble des interventions ponctuelles mues par ou à l'initiative de l'autorité administrative compétente aux fins de garantir le fonctionnement harmonieux et conforme à l'intérêt général d'une activité sociale » (F. JONGEN, *La police de l'audiovisuel. Analyse comparée de la régulation de la radio et de la télévision en Europe,* Bruxelles, bruylant, L.G.D.J., Paris, 1994, p. 50.

incompatible avec les articles 8 et 9 de la convention [n° 108] »[1202], prônant dès lors que le texte soit revu, ce qui n'a pas été fait.

C'est la raison pour laquelle d'aucuns soutiennent notamment que la loi du 8 décembre 1992 devrait limiter davantage le champ d'application de ces exceptions, suivant le modèle portugais, italien ou encore britannique[1203]. On pourrait prévoir qu'elles ne puissent être invoquées que lorsque les finalités concrètes ou la nature des données utilisées le justifient. Il reviendrait à l'autorité publique d'établir, dans chaque cas d'espèce, la légalité des exceptions invoquées[1204].

II. Une procédure d'accès à simplifier

338.- Un droit d'accès rarement exercé. De manière générale, les administrations reçoivent très peu de demandes d'accès fondées sur la loi du 8 décembre 1992.

> En guise d'illustration, l'INASTI, le SPF Finances et le Service public Wallonie n'ont reçu qu'une seule demande d'accès : la nôtre, effectuée pour les besoins de la présente recherche[1205]. Quant à l'ONSS, à la question « combien de demandes d'accès effectuées sur la base de la loi du 8 décembre 1992 avez-vous reçues ? », la réponse donnée fut « l'Office national de Sécurité sociale ne sait malheureusement pas répondre à cette question »[1206]. Après discussion, il s'avère qu'aucune demande de ce type ne leur a jamais été adressée.
>
> Cette situation est d'autant plus surprenante que ce droit d'accès existe depuis 1992 et que les administrations dont question sont bien connues des citoyens, qui traitent de nombreuses données à caractère personnel[1207].

Un tel constat interroge l'organisation de ce droit d'accès. En particulier, on se demande si la rareté des demandes d'accès n'est pas causée par

---

[1202] Avis de la section de législation du Conseil d'État du 28 novembre 1990 au sujet du projet de loi relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel, *Doc. parl.*, Ch. repr., sess. 1990-1991, n° 1610/1, pp. 57 et 58.

[1203] Pour de plus amples détails à ce sujet, voy. B. HAVELANGE et Y. POULLET, « Secret d'État et vie privée : ou comment concilier l'inconciliable ? », *op. cit.*, pp. 225-234.

[1204] *Ibid.*, pp. 232 et 233.

[1205] Ce constat a été dressé au mois d'août 2011.

[1206] Courriel de l'ONSS du 7 novembre 2011.

[1207] Le même constat semble devoir être fait en France. Sophie Vulliet-Tavernier, Directice des affaires juridiques à la CNIL, regrette ainsi que le droit d'accès aux données à caractère personnel est « soit trop souvent méconnu, soit peu exercé ». (voy. S. VULLIET-TAVERNIER, « La protection de la vie privée dans le cadre de l'administration électronique », *in Droit de l'administration électronique. Des nouveaux droits pour les usagers. Des nouvelles règles pour les agents,* Bruxelles, Bruylant, 2011, p. 167.

les embûches auxquelles sont confrontées les personnes intéressées par le traitement de leurs données.

Cette question retient l'attention. La rareté des demandes d'accès fondées sur la loi du 8 décembre 1992 risque d'induire, au sein des administrations, l'idée que les traitements de données ne sont pas contrôlés et que les abus n'entraîneront pas de sanctions. Pour les citoyens, les difficultés d'accès peuvent générer une certaine frustration, qui amplifie encore davantage la méfiance à l'égard de l'administration et de l'opacité qui entoure son action.

A. Les embûches

339.- Un droit d'accès méconnu. On peut raisonnablement penser que la rareté des demandes d'accès est un symptôme de la méconnaissance, par les citoyens, de la loi du 8 décembre 1992 en général, et du droit d'accès aux donnés à caractère personnel, en particulier. Un effort de publicité et de pédagogie devrait être initié, en menant davantage de campagnes d'informations à destination du grand public, par exemple[1208].

340.- Un droit d'accès laborieux. La procédure à initier est de nature à décourager un citoyen souhaitant simplement exercer sa curiosité légitime à l'égard du traitement de ses données par l'administration.

En effet, pour connaître les données que détient l'administration à son sujet, ainsi que l'usage qui en est fait, le citoyen doit prendre la peine de rédiger une lettre papier, photocopier le recto et le verso de sa carte d'identité, apposer un timbre qu'il doit lui-même payer, et poster le tout. Il peut introduire sa demande d'accès par courriel, mais doit pour ce faire être muni du dispositif nécessaire pour authentifier son courriel à l'aide d'une signature électronique. Une fois la demande introduite, il est contraint de patienter, l'administration disposant de 45 jours pour répondre[1209].

Par ailleurs, le demandeur d'accès ignore généralement quelle institution détient des données à son sujet. Pour connaître les traitements de ses données, il doit bien souvent introduire sa demande d'accès « à l'aveugle », sans savoir si une réponse intéressante sera fournie.

Plus encore, quand bien même il aurait connaissance de la localisation de ses données, l'administré risque d'éprouver des difficultés pour identifier le responsable de traitement à qui la demande doit être adressée. En ce sens, le médiateur fédéral affirme, à propos de l'utilisation d'une donnée à

[1208] Voy. *infra,* n°s 583.- et s.
[1209] Art. 10, §1, al. 2, de la loi du 8 décembre 1992.

caractère personnel erronée dans une décision administrative, que « trouver où et comment l'erreur a été commise revient presque à chercher une aiguille dans une botte de foin »[1210].

341.- Une surcharge de travail administratif. L'administration semble également découragée par le droit d'accès tel qu'organisé par la loi du 8 décembre 1992.

Certaines administrations ne connaissent pas, ou fort peu, l'existence de ce droit d'accès. Elles ne savent dès lors pas comment réagir aux demandes formulées dans ce cadre.

> Par exemple, en recevant notre demande d'accès, une administration nous a téléphoné pour savoir ce que l'on souhaitait, avouant ne pas comprendre notre lettre, alors qu'elle était rédigée à partir du formulaire type précité rédigé par la CPVP.

Plus généralement, la réponse à une demande d'accès constitue une charge importante de travail pour le fonctionnaire assigné à cette tâche. Plusieurs raisons fondent ce constat.

Certaines administrations disposent d'un très grand nombre de données pour chaque citoyen. La réponse à la demande d'accès requiert donc l'énoncé d'une grande quantité d'informations.

> C'est le constat auquel aboutit par exemple l'INASTI, qui détient à propos des travailleurs indépendants nombre de données issues du Registre national, des données relatives à l'affiliation à une caisse d'assurance sociale, des données relatives aux revenus perçus provenant du SPF Finances, des données carrière communiquées par la caisse d'assurance sociale, des données relatives à l'encodage du dossier par l'INASTI, etc. Bien que cette administration soit de très bonne volonté, les données de détail ne sont pas communiquées[1211], pour que la réponse au droit d'accès demeure compréhensible.

Le travail imposé à l'administration sollicitée est d'autant plus conséquent qu'elle ne peut se contenter d'envoyer au demandeur la copie, telle quelle, des informations reprises dans sa base de données. En effet, la loi du 8 décembre 1992 exige que la communication des données soit effectuée « sous une forme intelligible »[1212]. En outre, rappelons que le citoyen peut demander de connaître l'origine des données, la finalité du traitement de chacune d'elles, l'identification des destinataires.

[1210] Médiateur fédéral, *Rapport annuel 2010*, p. 90.

[1211] Néanmoins, nous n'avons pas eu d'explication sur ce qu'on entend par données de détail.

[1212] Art. 10, al. 1, b), de la loi du 8 décembre 1992.

Ces exigences aboutissent à assortir chaque information traitée de nombreuses explications afin de rédiger une réponse compréhensible par tout citoyen. Cette tâche monopolise un temps certain et ce d'autant plus qu'à l'heure actuelle, il n'existe pas de directive fournies aux administrations pour rédiger les réponses aux demandes d'accès[1213].

B. Des pistes de solution

342.- Des outils de transparence. Certaines administrations bénéficient d'outils qui permettent d'atténuer les difficultés précédemment décrites et de conforter la transparence des traitements de données à caractère personnel. On pense au répertoire des références de la Banque-Carrefour de la sécurité sociale, et aux accès directs aux données du Registre national.

§1. Le répertoire des références

343.- Un outil pour localiser les données. Comme cela a été détaillé précédemment[1214], le répertoire des références contient notamment une table, dénommée « répertoire des personnes », reprenant, pour chaque citoyen, la référence des institutions de sécurité sociale possédant un dossier à leur nom.

Le citoyen a la possibilité de s'adresser à la Banque-Carrefour de la sécurité sociale pour obtenir l'extrait de cette table qui le concerne. Concrètement, le demandeur reçoit la liste des institutions qui gèrent un dossier le concernant, mais non les données elles-mêmes. À partir de cette liste, la personne concernée est en mesure d'identifier les administrations qui détiennent des données à son sujet et peut ainsi être incitée à exercer son droit d'accès sur la base de la loi du 8 décembre 1992.

Le répertoire des références et la possibilité pour tout citoyen d'en obtenir une copie pour les données qui le concernent présentent un intérêt particulier dans une administration structurée en réseaux. En effet, puisque, dans un réseau sectoriel, les administrations s'échangent les informations, il peut être difficile pour la personne concernée d'identifier l'origine des données utilisées, et le responsable du traitement de celles-ci. Le répertoire de référence constitue un outil utile pour lui permettre d'orienter ses demandes d'accès, et, de cette manière « éviter que le citoyen soit

[1213] Constat dressé en novembre 2011 suite à des entretiens avec des fonctionnaires émanant d'administrations fédérales et régionales.

[1214] Voy. *supra,* n° 25.-

découragé d'exercer ses droits parce qu'il lui est impossible d'identifier le(s) bon(s) interlocuteur(s) »[1215].

344.- L'obtention d'un extrait du répertoire de référence. Pour obtenir l'extrait du répertoire des références qui le concerne, le citoyen doit introduire une demande d'accès auprès de la Banque-Carrefour de la sécurité sociale, qui respecte les exigences précédemment énoncées.

> Signalons que le site de la Banque-Carrefour de la sécurité sociale met à disposition du citoyen un formulaire intitulé « Demande de communication de données à caractère personnel par la Banque-Carrefour de la sécurité sociale »[1216].

On regrette à nouveau la lourdeur de cette procédure, encore renforcée par la complexité du site de la Banque-Carrefour de la sécurité sociale qui ne mentionne pas clairement la possibilité d'obtenir cet extrait du répertoire des références, ni l'existence d'un formulaire en cette matière. La procédure gagnerait à être simplifiée en permettant aux citoyens d'introduire la demande via une rubrique claire du site internet, et une identification par la carte d'identité électronique.

En outre, la copie de l'extrait du répertoire des références devrait mentionner, pour chaque institution de sécurité sociale y reprise, les données de la personne à contacter pour obtenir des renseignements sur les données détenues par l'institution de sécurité sociale.

§2. L'accès direct aux données

345.- Un outil de consultation des données. Tout citoyen peut accéder directement, en ligne, à ses données détenues au Registre national selon une procédure exposée ci-après.

Ce type d'accès encourage les citoyens à exercer leur droit d'accès et les incite ainsi à veiller à l'utilisation de leurs données à caractère personnel par les administrations ayant accès au Registre national. De toute évidence, il est plus aisé et agréable de surfer gratuitement sur un site internet que de s'astreindre à rédiger un courrier nécessitant que l'on se renseigne sur les éléments à y intégrer précisément, que l'on identifie la personne à qui l'adresser, que l'on paie un timbre et pense à poster ce courrier. Par ailleurs, l'accès électronique facilite aussi le travail de l'administration qui

[1215] CPVP, recommandation n° 03/2009, *op. cit.*, p. 6.

[1216] Ce formulaire est disponible à l'adresse http://www.ksz-bcss.fgov.be/binaries/documentation/fr/faq/formulier_artikel_10_wvp_fr.pdf

n'est pas contrainte de répondre aux courriers relatifs au droit d'accès, évitant ainsi la surcharge de travail évoquée précédemment.

Pour ces raisons d'ailleurs, la CPVP encourage la mise en place de tels accès électroniques[1217], soutenant que « la procédure d'accès électronique est non seulement respectueuse de la vie privée mais peut également aider l'administration concernée à mieux gérer sa charge de travail et à détecter un abus de données »[1218]. À l'occasion de l'organisation de l'échange électronique des données administratives en Flandre, la CPVP a même suggéré de « prévoir la possibilité pour le citoyen de contrôler électroniquement ses données dans des sources authentiques. Ceci requiert évidemment [...] qu'une authentification valable soit exigée afin de garantir que le citoyen ne puisse consulter que ses propres données »[1219]. Progressivement d'autres administrations mettent en place cet outil. Ainsi le citoyen peut-il, à l'heure actuelle, bénéficier du système Mypension, lui permettant de consulter son dossier pension en ligne[1220] ainsi que de Myminfin, qui permet l'accès au dossier fiscal[1221].

L'accès direct électronique au Registre national est organisé par l'article 6, §3, de la loi du 19 juillet 1991[1222].

> Concrètement, cet accès s'exerce en se connectant sur le site https://mondossier.rrn.fgov.be/Le demandeur d'accès doit s'identifier à l'aide de sa carte d'identité et d'un lecteur de carte. Signalons d' ailleurs que certaines communes offrent gratuitement des lecteurs de carte aux administrés.

En se connectant au portail « Mon dossier », la personne concernée accède à deux types d'informations : les données de contenu détenues par le Registre national, ainsi que les données de consultation.

[1217] CPVP, avis n° 41/2008 du 17 décembre 2008 relatif à une demande d'avis concernant l'avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de Services fédéral, p. 16, n° 75 ; avis n° 23/2008 du 11 juin 2008, relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules, p. 36, n° 121.

[1218] CPVP, avis n° 23/2008 précité.

[1219] CPVP, avis n° 11/2009 du 29 avril 2009 concernant le projet d'arrêté du Gouvernement flamand portant exécution du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, p. 6.

[1220] Via le site http://www.onprvp.fgov.be/fr/about/pages/mypension.aspx

[1221] Via le site http://ccff02.minfin.fgov.be/portal/portal/MyMinfinPortal/welcome

[1222] Loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la li du 8 août 1983 organisant un Registre nation des personnes physiques, *M.B.,* 3 septembre 1991.

1. Les données de contenu

346.- La consultation des données. Le citoyen peut consulter les données et les types d'informations y relatives détenues à son sujet dans la source authentique qu'est le Registre national. Ainsi sont repris ses nom, prénoms, date de naissance, adresse mais également la profession, des données relatives à son permis de conduire, à sa participation aux élections, etc. En outre, une rubrique est consacrée aux informations propres au statut d'étranger. Une personne dans cette situation y trouvera notamment les données relatives à son permis de travail, au CPAS qui en a la charge, etc.

347.- La rectification des données. Par ailleurs, le portail mentionne clairement la possibilité pour la personne d'exercer son droit de rectification auprès de sa commune, si une erreur est constatée affectant ses données à caractère personnel[1223]. L'exercice du droit de rectification est facilité par la présence d'un hyperlien contenant l'adresse mail de la commune.

348.- L'obtention de documents. Enfin, une rubrique « transactions » permet au citoyen d'obtenir les documents officiels reprenant ses données tels qu'une composition de ménage, un certificat de nationalité, un extrait de registre de la population, ou de créer lui-même un document en sélectionnant les données qui doivent s'y trouver.

2. Les données de consultation

349.- L'historique des consultations. Une autre particularité intéressante du portail « Mondossier » est la rubrique « Historique des consultations », qui permet à la personne concernée de connaître, en principe, « toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consulté ou mis à jour ses données au registre de la population ou au registre national des personnes physiques »[1224].

[1223] La procédure est réglée par l'annexe 1er de la ccirculaire du 23 juin 2008 relative à l'application de l'arrêté royal du 19 mars 2008 organisant la procédure de communication des différences constatées entre les informations du Registre national des personnes physiques et celles des registres visés à l'article 2 de la loi du 8 août 1983 organisant un Registre national des personnes physiques, publié au Moniteur belge du 15 avril 2008.

[1224] Art. 6, §3, 3°, de la loi du 19 juillet 1991 précitée. Voy. égal. l'arrêté royal du 13 février 2005 déterminant la date d'entrée en vigueur et le régime du droit de prendre connaissance des autorités, organismes et personnes qui ont consulté ou mis à jour les informations reprises dans les registres de population ou au registre national des personnes physiques, *M.B.,* 28 février 2005.

350.- Les finalités poursuivies. Deux finalités justifient l'enregistrement des données de consultation. D'une part, il s'agit d'assurer la protection de la vie privée des citoyens en leur permettant de savoir qui a consulté leurs données. D'autre part, cette mesure vise à « permettre au citoyen de jouer un rôle d'avertisseur, puisqu'il est le mieux placé pour détecter des consultations 'anormales' pouvant donner lieu à des sanctions »[1225].

351.- Le contenu des données de consultation. En accédant au portail « Mondossier », le citoyen se trouvera confronté à ce type de tableau reprenant la commune ou l'organisme ayant consulté les données, ainsi que des informations plus générales.

Décembre 1/1[1226]

Date/heure	INS	Commune/Organisme	Code	Transaction
2011-12-15 10 :27 :25	092114	ADM. COM. DE SOMBREFFE	FO	Consultation photo

a) L'organisme ayant consulté les données. Des réflexions ont récemment été menées pour savoir s'il était nécessaire de détailler les données de consultation au point de faire figurer le nom de l'agent qui a accédé aux données. Jusqu'il y a peu, c'est ce que mentionnait l'historique des consultations, en reprenant le numéro d'identification du Registre national de l'agent.

Depuis lors, la CPVP soutient qu'une telle précision est excessive par rapport aux finalités de l'enregistrement des données de consultations qui viennent d'être énoncée.

> Selon la CPVP, « le citoyen ne peut tirer aucune conclusion quant au motif et à la régularité d'une consultation sur la seule base du nom du fonctionnaire ayant effectué celle-ci. Dès lors, [...] la communication du nom de l'agent doit être considérée comme excessive au regard de l'article 4, §1, 3°, de la [loi du 8 décembre 1992] »[1227].

[1225] CPVP, avis n° 12/2009 du 29 avril 2009 relatif à une demande d'avis émanant du SPF Intérieur concernant un certain nombre de questions qui se sont posées dans la délibération RN n° 19/2008, p. 6.

[1226] Ceci est la copie de l'une des informations auxquelles nous avons été confrontées en exerçant notre droit d'accès. Comme on peut le constater, toutes ces données ne sont pas compréhensibles.

[1227] CPVP, avis n° 12/2009 précité, p. 7. Dans le même sens, voy. CPVP, recommandation n° 03/2010 du 9 juin 2010 relative à l'application des « circles of trust » (cercles de confiance) et à l'obligation de transparence concernant les consultations des informations du Registre national, p. 4, n° 11.

Concrètement, les données de consultation doivent contenir suffisamment d'informations pour que la personne concernée puisse trouver aisément le bon interlocuteur si elle souhaite connaître davantage d'informations, telles que, notamment, la finalité de la consultation des données. C'est pourquoi, il est conseillé de désigner le service administratif au départ duquel la consultation est intervenue ainsi que la personne de contact qui peut être sollicitée pour obtenir davantage d'informations[1228].

Parallèlement à ce qui figure dans l'application « Mondossier », les administrations dont les agents ont accès au Registre national doivent disposer, en interne, d'un système qui enregistre l'identité des fonctionnaires chaque fois qu'ils effectuent une consultation de la source authentique. Un tel système est indispensable pour plusieurs raisons[1229].

Il permet à l'autorité de contrôler ses agents, notamment si une augmentation anormale de consultations est constatée en provenance de l'un d'eux.

En outre, si un citoyen demande des éclaircissements à propos d'une consultation en particulier, ce système est nécessaire pour demander à l'agent concerné les précisions requises.[1230]

Enfin, le fait, pour les fonctionnaires, de savoir que leur identité est enregistrée et qu'il existe dès lors une possibilité de contrôler leurs actes en ce domaine est de nature à les inciter à faire bon usage du Registre national.

b) Les autres informations. « Mondossier » mentionne également la date et l'heure de la consultation, ainsi que des informations plus obscures, à savoir, l' « INS », le « Code » et la « transaction ». Malheureusement, ces termes ne sont pas définis et il est difficile d'accéder à leur signification. Le portail « Mondossier » gagnerait à être enrichi d'une explication de ces données, accessibles aisément. En particulier, il faudrait veiller à indiquer la finalité poursuivie par la consultation de manière précise et compréhensible.

Pour l'heure, il y a lieu de chercher dans le site internet du Registre national les documents pertinents à ce sujet. On trouve ainsi dans la rubrique « Instructions », un formulaire relatif aux « instructions pour la tenue à jour des informations », dont l'annexe n° 3 donne la traduction des « codes d'interrogation ». Malheureusement, celle-ci est elle-même peu compréhensible. Elle semble également incomplète puisque nous n'avons pu y trouver la traduction du code FO repris dans l'exemple précité.

[1228] CPVP, avis n° 12/2009 précité, p. 7.

[1229] *Ibid.*, p. 8.

[1230] Au sujet de la possibilité d'obtenir le nom de l'agent qui a consulté les données, voy. *infra,* n° 404.-

Section 3. La publicité active des traitements de données à caractère personnel

352.- Considérations générales. Une obligation d'information active s'impose aux administrations qui ont la qualité de responsable de traitement. Cette obligation est néanmoins assortie d'exceptions, dont certaines bénéficient à de nombreuses administrations.

I. L'obligation d'information

353.- Une exigence cardinale. L'obligation d'information est une « pierre angulaire »[1231] de la loi du 8 décembre 1992. En effet, comme cela a été dit précédemment, la visibilité des traitements de données effectués au sein de l'administration est moindre aujourd'hui qu'hier, en raison du fait, notamment, que les citoyens ne doivent plus fournir plusieurs fois les mêmes informations aux administrations. Il faut pourtant veiller à ne pas mettre les intéressés à l'écart de l'action administrative. En ce sens, partant du constat qu'à l'heure du développement de l'e-gouvernement, le pouvoir de l'administration est renforcé par les technologies, la CPVP soutient qu'« il est effectivement indispensable qu'une réciprocité des avantages soit mise sur pied »[1232], en veillant à l'effectivité des droits des personnes concernées[1233].

Dans ce contexte, l'obligation d'information vise à permettre aux personnes concernées de connaître, sans devoir les réclamer, les éléments essentiels des traitements « comme c'était traditionnellement le cas lors de la demande séparée de données »[1234]. Il s'agit également d'un moyen de sensibiliser les individus à la matière, en leur permettant de comparer les pratiques de chaque institution et éventuellement de dénoncer celles qui paraissent abusives[1235].

[1231] CPVP, avis n° 15/2006 du 14 juin 2006 relatif au projet d'arrêté royal réglant la collaboration à l'association chargée de l'enregistrement du kilométrages des véhicules, p. 19, n° 73.

[1232] CPVP, avis n° 01/2007, *op. cit.,* p. 15, n° 83.

[1233] Sur le principe de la réciprocité des avantages voy. *infra,* n°s 382.- et s.

[1234] CPVP, avis n° 22/2005 du 21 décembre 2005 relatif à un avant-projet d'arrêté du Gouvernement wallon modifiant le Code de l'eau [...], p. 7, n° 21.

[1235] Rapport de l'OCDE n° DSTI/ICCP/REG(2006)5/FINAL, « Simplifier les notices d'information sur la protection de la vie privée : rapport et recommandation de l'OCDE », disponible en ligne sur le site http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2006)5/FINAL&docLanguage=Fr

La loi du 8 décembre 1992 organise les modalités de l'obligation d'information. Elle prévoit également des exceptions à ce devoir.

A. Le principe de l'obligation d'information

354.- Considérations générales. L'administration qui effectue des traitements de données doit fournir spontanément aux personnes concernées un certain nombre d'informations déterminées par la loi du 8 décembre 1992. Elle doit veiller à le faire d'une manière compréhensible et en temps opportun, conformément à la loi du 8 décembre 1992.

§1. Le contenu de l'information

355.- L'article 9 de la loi du 8 décembre 1992. L'article 9, §§1 et 2, de la loi du 8 décembre 1992 dresse une liste d'informations à fournir. Certaines sont obligatoires, d'autres, facultatives. D'autres encore ne s'imposent que si elles sont déterminées par le Roi.

a) Les informations obligatoires. Toute personne concernée par un traitement de données a toujours le droit de connaître les informations suivantes :

> « a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;
>
> b) les finalités du traitement ;
>
> c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de *direct marketing* »

b) Les informations « supplémentaires ». À ces informations obligatoires, s'ajoutent des informations « supplémentaires », qui ne doivent être fournies que « dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires [sont nécessaires] pour assurer à l'égard de la personne concernée un traitement loyal des données ». La loi du 8 décembre 1992 en dresse une liste non exhaustive qui diffère quelque peu selon que les données sont fournies directement par le citoyen, ou non.

> Lorsque les données sont fournies directement par le citoyen, l'article 9, §1, de la loi du 8 décembre 1992 prévoit que peuvent être communiquées :
>
> « d) d'autres informations supplémentaires, notamment :
>
> – les destinataires ou les catégories de destinataires des données,

– le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse, l'existence d'un droit d'accès et de rectification des données la concernant »

Lorsque les données ne proviennent pas directement du citoyen l'article 9, §2, de la loi du 8 décembre 1992 prévoit que peuvent être communiquées :

« d) d'autres informations supplémentaires, notamment :

– les catégories de données concernées ;

– les destinataires ou les catégories de destinataires ;

– l'existence d'un droit d'accès et de rectification des données la concernant »

En d'autres termes, il revient aux administrations d'apprécier si la loyauté du traitement suppose que ces informations supplémentaires soient fournies. Compte tenu de ce large pouvoir d'appréciation, il serait judicieux d'établir des lignes de conduite à ce sujet afin de faciliter le travail administratif tout en respectant le droit d'information des personnes concernées.

Pour l'heure, la CPVP soutient que des informations supplémentaires doivent en tout cas être fournies lorsque les données sont utilisées par un intégrateur de services, ou lorsqu'elles peuvent avoir des conséquences lourdes sur la personne concernée.

Comme cela a été établi dans le premier titre de la recherche, les données collectées sont de plus en plus souvent intégrées dans un réseau sectoriel comprenant, en son cœur, un *intégrateur de services* chargé d'assurer la circulation des données entre les administrations du réseau. En raison des échanges d'informations entre administrations, le citoyen n'est plus contacté et n'aperçoit plus d'emblée l'utilisation faite de ses informations. Pour cette raison, la CPVP recommande de publier « des informations claires concernant toutes les facettes du fonctionnement [de l'intégrateur de services], de manière à ce que chacun ait la possibilité de vérifier la régularité de son intervention ». Ainsi, il faut « définir et expliquer le but de l'intégration de services. Cette finalité est en effet le critère sur la base duquel on établit si son traitement est réellement lié à la finalité ». Il y a lieu également d' « indiquer clairement quels services il agrège [et] quels traitements il exécute »[1236].

Par ailleurs, le traitement de certaines données peut avoir des *conséquences lourdes* sur la situation de la personne concernée. On pense notamment aux données utilisées dans l'appréciation du droit à une allocation. La CPVP soutient que, dans une telle hypothèse, « il est essentiel que

[1236] CPVP, recommandation n° 03/2009, *op. cit.,* p. 9, n° 33. Voy. également CPVP, avis 14/2010 du 31 mars 2010 sur un avant-projet de loi portant création de la Banque-Carrefour des permis de conduire, p. 7, n° 28.

l'attention de la personne concernée soit attirée sur son droit d'accès et de rectification »[1237].

c) Les informations déterminées par le Roi. La loi du 8 décembre 1992 habilite le Roi à déterminer encore d'autres informations à fournir « en fonction du caractère spécifique du traitement, après avis de la commission de la protection de la vie privée ».

§2. Le mode de communication de l'information

356.- Des informations précises et compréhensibles. Il importe de communiquer aux citoyens des informations précises et compréhensibles sur les traitements de leurs données. Le plus généralement, cela se fait à partir d'un document dénommé « Notice d'information relative à la protection de la vie privée » ou un onglet « Privacy » sur le site internet de l'institution. Néanmoins, la rédaction d'une notice de qualité n'est pas chose aisée, tant les informations à fournir sont nombreuses, et le jargon utilisé souvent complexe.

L'importance de l'information relative à la protection des données et le souci d'en améliorer la lisibilité ont d'ailleurs été reconnus au niveau international. Plusieurs initiatives ont déjà été concrétisées en ce domaine.

> Par exemple, le commissariat à l'information du *Royaume-Uni* a publié en 2007 un rapport intitulé « Fair Processing Notifications »[1238] qui atteste que 60 % des citoyens sont sensibles à l'utilisation faite de leurs données mais que la plupart d'entre eux ignorent les notices d'information relatives à la protection des données à caractère personnel ou ne les comprennent pas.
>
> Aux *États-Unis*, des initiatives gouvernementales ont également été lancées, dont plusieurs enquêtes menées auprès des citoyens afin d'évaluer l'efficacité des notices d'information[1239].
>
> En 2003, la 25e *Conférence internationale des commissaires pour la protection des données* a abouti à une résolution pour améliorer la communication au

[1237] CPVP, avis n° 30/96 du 13 novembre 1996 concernant un avant-projet de loi adaptant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel à la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, p. 15, n° 26.

[1238] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ic_final_report_version_1.1_final.pdf

[1239] La conclusion de ces enquêtes est publique. Voy. http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf

sujet des pratiques concernant la protection des données[1240]. Cette résolution a ensuite été confirmée par un protocole d'accord suite à des discussions menées entre experts de la protection de la vie privée issus des secteurs public et privés à Berlin en 2004[1241].

La même année, le groupe de travail européen sur la protection des données, dénommé « Groupe de l'article 29 », a rendu un avis à ce sujet[1242].

L'*OCDE* a également consacré nombre de travaux à cette question, et a notamment rédigé, en 2006, un rapport qui comprend diverses recommandations intitulé « Simplifier les notices d'information sur la protection de la vie privée »[1243].

357.- Les notices d'informations multistrates. Il ressort de ces études et accords internationaux que les notices d'informations gagneraient à être structurées suivant un format à plusieurs niveaux, dit également « format multistrates »[1244].

En somme, il s'agit de communiquer au citoyen une *notice d'information courte*, simple et compréhensible, reprenant les renseignements les plus importants pour comprendre les traitements auxquels ses données sont soumises. Cette notice courte doit être diffusée d'une manière telle que le citoyen ait l'attention attirée sur celle-ci. On pense notamment à un affichage très visible sur le site internet de l'institution.

Cette notice courte doit contenir un renvoi à la *déclaration complète* comprenant en détails, toutes les informations relatives aux traitements de données effectués par l'institution qui en est responsable. Cette déclaration doit notamment mentionner clairement un point de contact pour les questions et les renseignements ainsi que les recours possibles. Il est recommandé de placer ces informations dans un tableau, pour faciliter la lecture rapide des informations[1245].

[1240] http://www.privacyconference2003.org/pdf/Resolution_on_Privacy_Information_Practices.doc

[1241] http://www.hunton.com/files/tbl_s47Details/FileUpload265/681/Berlin_Workshop_Memorandum_4.04.pdf

[1242] Groupe 29, avis 10/2004 sur « Dispositions davantage harmonisées en matière d'informations », 25 novembre 2004, WP 100 disponible sur le site http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_fr.pdf

[1243] hhttp://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2006)5/FINAL&docLanguage=Fr

[1244] http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2006)5/FINAL&docLanguage=Fr, p. 6.

[1245] Groupe 29, avis 10/2004 précité, p. 10.

Un exemple pertinent de notice d'information multistrates peut être trouvé sur le site de la poste américaine, *United States Postal Service*[1246].

La CPVP a déjà émis des suggestions en ce sens. Ainsi, en 1997 affirmait-elle déjà que « l'Internet offre une possibilité technique aisée et très légère de concrétiser cette obligation. Il suffirait de demander aux maîtres de fichiers qui collectent des données à caractère personnel via l'Internet, au moment où ils informent les personnes sur leurs droits vis-à-vis des données collectées, d'inclure [...] un « hyperlien » vers leur déclaration telle qu'elle se trouve enregistrée dans le registre public. La personne qui répond au formulaire qui lui est proposé pourrait ainsi, d'un simple « click », être transportée sur le site Internet de la Commission où lui sera montrée la déclaration relative au traitement dont question et au maître du fichier qui l'interroge »[1247].

§3. Le moment de communiquer l'information

358.- Collecte directe et collecte indirecte des données. Selon que les données sont collectées directement auprès de la personne concernée, ou non, les informations ne doivent pas être communiquées au même moment.

Pour être tout à fait précis, il y lieu de souligner que l'article 9 de la loi du 8 décembre 1992 use des termes « obtention » des données, et non « collecte ». Selon les travaux préparatoires, « l'expression 'obtenir des données auprès de la personne concernée' vise également la situation dans laquelle la personne concernée communique spontanément des données à caractère personnel au responsable du traitement, par exemple, lors [...] de la demande d'une prime au guichet de la maison communale ». « Il s'agit bien ici d' 'obtenir' des données au sens large et non pas uniquement [...] de 'collecter' des données à caractère personnel d'une façon active »[1248].

Néanmoins, dans la présente recherche, le terme « collecte » s'entend de manière large, pour viser toutes les hypothèses dans lesquelles les données ont été fournies directement par la personne concernée ou indirectement par une autre administration.

[1246] http://about.usps.com/who-we-are/privacy-policy/privacy-policy-highlights.htm

[1247] CPVP, avis n° 36/97 du 27 novembre 1997 relatif au projet d'arrêté royal (n° 18) fixant les modalités d'accès au registre public des traitements automatisés de données à caractère personnel prévu à l'article 18 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, p. 9.

[1248] Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Doc. Parl.*, Ch. repr., session 1997-1998, n° 1566/1, p. 44.

359.- Collecte directe. En vertu de l'article 9, §1, de la loi du 8 décembre 1992, l'information doit se faire au plus tard au moment de la collecte effectuée directement auprès de la personne concernée.

De manière générale, cette information prend la forme d'une clause intégrée dans le formulaire que doit remplir la personne concernée, tel que le formulaire de déclaration des revenus[1249]. La CPVP encourage le responsable de traitement à faire un renvoi, dans ce formulaire, à un site internet reprenant une information plus complète, conformément à la méthode de la notice multistrates décrite précédemment[1250].

360.- Collecte indirecte. L'obligation d'information en cas de collecte indirecte des données est organisée par l'article 9, §2, de la loi du 8 décembre 1992.

> La CPVP a précisé les trois situations dans lesquelles cette disposition trouve application, à savoir « 1. lorsqu'un responsable veut utiliser des données à caractère personnel pour d'autres finalités que celles prévues au moment de la collecte ou du premier enregistrement ; 2. lorsqu'un responsable envisage la communication de données à caractère personnel à des tiers pour d'autres finalités que celles prévues au moment de la collecte ou du premier enregistrement ; 3. au moment du premier enregistrement de données qui n'ont pas été collectées auprès de la personne concernée »[1251]. La CPVP avait d'ailleurs demandé que ces précisions soient inscrites dans la loi du 8 décembre 1992, ce qui n'a pas été fait.

Dans cette hypothèse, l'information s'effectue au moment de l'enregistrement des données obtenues indirectement. En outre, « si une communication de données à des tiers est envisagée », l'information doit être fournie « au plus tard au moment de la première communication de données »[1252].

[1249] CPVP, avis n° 22/95 du 27 juin 1995 relatif au respect de l'article 4 de la loi du 8 décembre 1992 par l'Administration des Contributions Directes lors de l'envoi des déclarations d'impôts des personnes physiques, p. 2, n° 3 ; avis n° 27/2007 du 19 septembre 2007 relatif à l'échange de données à caractère personnel entre administrations fiscales – vérification fiscale subséquente aux demandes de remboursement de la taxe sur les opérations boursières illégalement perçue suite à l'arrêt de la Cour de justice des Communautés européennes du 15 juillet 2004, p. 6, n° 32 ; CPVP, avis n° 07/2010 du 17 mars 2010 relatif à un projet d'accord de coopération entre les Centres publics d'action sociale et l'Office du travail de la Communauté germanophone, p. 10, n° 26.

[1250] CPVP, avis n° 06/2009 du 18 mars 2009 relatif à un avant-projet de loi portant création de la Source authentique des données relatives aux véhicules, p. 9, n° 22.

[1251] CPVP, avis n° 30/96 précité, p. 15, n° 27.

[1252] Art. 9, §2, de la loi du 8 décembre 1992.

Cette disposition laisse perplexe. En effet, l'intérêt d'informer la personne concernée de la réutilisation de ses informations réside principalement dans la possibilité pour cette dernière d'exercer un recours en opposition, s'il refuse que ses données soient transmises d'une administration à une autre. Or, l'information concernant la transmission des données peut n'être faite qu'au moment où les données sont effectivement réutilisées. Concrètement, cela signifie que le citoyen ne pourra s'opposer à la réutilisation de ses données qu'une fois les données déjà transmises. En outre, il recevra, quasiment au même moment, la même information de la part des deux institutions concernées : celle qui émet les données, au moment de la transmission et celle qui les a reçues, au moment où elle les enregistre. La CPVP avait d'ailleurs soulevé la question au moment de la modification, en 1998, de la loi du 8 décembre 1992. Elle a dit se demander « si l'information atteint son but [...] si on attend jusqu'au moment de la transmission. Le droit d'opposition devient alors un faux droit. La personne concernée devrait pouvoir s'opposer à cette communication même »[1253].

B. Les exceptions à l'obligation d'information

361.- Considérations générales. La loi du 8 décembre 1992 prévoit que dans certaines hypothèses, l'administration responsable des traitements de données est dispensée du devoir d'informer les personnes concernées. En particulier, deux exceptions retiennent notre attention dans le cadre de cette recherche. Il s'agit de l'exception liée au fait que les personnes concernées ont déjà connaissance des informations et celle applicable lorsque la collecte indirecte des données est prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

§1. La personne concernée a déjà connaissance des informations

362.- L'article 9, §§1 et 2, alinéa 1, de la loi du 8 décembre 1992. Que les données soient obtenues directement, ou non, l'administration ne doit pas communiquer à la personne concernée les informations relatives au traitement si cette dernière « en est déjà informée »[1254].

Cette exception doit s'entendre de manière stricte. Elle ne peut valoir que s'il est certain que la personne concernée dispose déjà de toutes ces informations et non s'il s'agit seulement d'une supposition.

[1253] CPVP, avis n° 30/96 précité, p. 16, n° 28.
[1254] Art. 9, §§ 1 et 2, al. 1, de la loi du 8 décembre 1992.

Partant de là, une administration peut-elle se prévaloir de la base légale sur laquelle se fonde sa compétence, pour ne pas informer la personne concernée au motif qu'elle est censée connaître la loi ? La négative s'impose, du moins en l'état actuel de la législation. En effet, comme l'a démontré le premier titre de la recherche, les lois sont particulièrement lacunaires s'agissant des traitements de données dans l'e-gouvernement. Quand bien même un citoyen aurait la patience nécessaire de les chercher, de les lire et de les comprendre, il n'y trouverait pas l'ensemble des informations auxquelles il a droit. Il revient donc à l'administration responsable du traitement de l'en informer.

> En ce sens, la CPVP a contredit le SPF Finances qui prétendait ne pas devoir informer les contribuables dans le formulaire de déclaration de revenus, justifiant son attitude « par la connaissance suffisante qu'aurait chaque contribuable de la base légale ou réglementaire de la collecte des données et des finalités qu'elle poursuit ». La CPVP a souligné que les citoyens ignorent les finalités poursuivies par le SPF Finances dans le cadre de cette collecte de données, tout comme ils n'ont pas connaissance des « nombreuses communications de données à caractère fiscal vers d'autres administrations »[1255].

§2. La collecte indirecte est effectuée par ou en vertu d'une loi, d'un décret ou d'une ordonnance

363.- L'article 9, §2, alinéa 2, b), de la loi du 8 décembre 1992. La loi du 8 décembre 1992 prévoit une exception à l'obligation d'information qui risque d'être invoquée de plus en plus souvent au gré du développement de l'e-gouvernement, amplifiant encore l'opacité de l'action administrative.

Cette exception est prévue à l'article 9, §2, alinéa 2, b) de la loi du 8 décembre 1992 et formulée comme suit :

> « Le responsable du traitement est dispensé de fournir les informations visées au présent paragraphe :
>
> b) lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.
>
> Le Roi détermine par arrêté délibéré en Conseil des ministres après avis de la Commission de la protection de la vie privée les conditions pour l'application de l'alinéa précédent »[1256].

[1255] CPVP, avis n° 22/95 précité, p. 2.

[1256] Le Roi a usé de cette habilitation législative pour organiser la mise en œuvre de cette exception dans un cas bien spécifique, lié au codage des données réutilisées à des fins statistiques, historiques et scientifiques. Ce point s'écarte du sujet de notre recherche. C'est

Cette exception est critiquable, en raison de sa contrariété avec la directive 95/46 et de l'interprétation qu'en fait la CPVP, comme l'expliquent les lignes qui suivent.

364.- L'article 11, §2, de la directive 95/46. L'article 11, §2, de la directive 95/46 formule l'exception en question comme suit :

> « Le paragraphe 1 ne s'applique pas lorsque [...] la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les États membres prévoient des garanties appropriées ».

La directive 95/46 subordonne donc l'exception au devoir d'information à la condition que l'enregistrement ou la communication des données aient été organisés par le législateur, à qui il revient de déterminer, notamment, la nature des données échangées, le type de traitement, etc. Or, la loi du 8 décembre 1992 prévoit que l'exception au devoir d'information peut être invoquée si l'enregistrement ou la communication des données est prévu « par ou en vertu d'une loi, d'un décret ou d'une ordonnance ». Cela signifie donc que les autorités administratives peuvent invoquer cette exception en se fondant uniquement sur une norme de valeur réglementaire prévoyant l'échange des données. En cela, la loi du 8 décembre 1992 offre aux administrés une protection plus faible que celle imposée par la directive 95/46[1257].

365.- L'interprétation de la CPVP. Cette exception est d'autant plus critiquable que la CPVP en donne une interprétation large.

La question se pose de savoir si l'exception visée à l'article 9, §2, alinéa 2, b), de la loi du 8 décembre 1992 s'applique uniquement dans l'hypothèse prévue à l'article 29 de l'arrêté royal précité, ou si elle peut être étendue à d'autres situations.

Dans un premier temps[1258], la CPVP a considéré que l'exception devait être interprétée strictement. Elle ne pouvait être invoquée que dans l'hypothèse visée à l'article 29 dudit arrêté royal. Ainsi, seules les autorités

---

pourquoi, nous ne l'approfondissons pas. Pour de plus amples détails, voy. l' arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.,* 13 mars 2001, p. 07839 et en particulier, l'article 29 qui se trouve dans le chapitre IV de cet arrêté royal, consacré aux « conditions pour l'exemption de l'obligation d'information visée à l'art. 9, §2, de la loi ».

[1257] En ce sens également, C. DE TERWANGNE, *Société de l'information et mission publique d'information*, *op. cit.*, pp. 265 et 598.

[1258] Voy. not. CPVP, avis n° 26/2006 du 12 juillet 2006 concernant l'utilisation d'images satellites afin de dépister et constater des infractions aux normes urbanistiques, p. 8, n° 20.

administratives chargées de rassembler et de coder des données pouvaient l'invoquer.

Depuis, la CPVP est revenue sur cette interprétation. Elle prône aujourd'hui une interprétation large de l'exception au devoir d'information, qui peut être invoquée vis-à-vis d'autres cas que celui visé à l'article 29 dudit arrêté royal.

Dans une note méthodologique sur laquelle les membres de la CPVP se sont accordés[1259], elle développe un raisonnement tortueux fondé sur l'article 11, §2, de la directive 95/46. En somme, puisque la directive prévoit que les États-membres doivent prendre des « garanties appropriées » pour encadrer l'exception, la CPVP considère que la tâche du Roi est de prévoir de telles garanties. Etonnamment, la CPVP considère que ces garanties sont déjà prévues par la loi ; cela n'a donc pas de sens d'imposer au Roi d'adopter des dispositions réglementaires qui se résumeraient à dire que la loi se suffit à elle-même. L'exception légale peut donc être invoquée dans d'autres hypothèses que celle visée à l'article 29 de l'arrêté royal.

Ainsi, la CPVP admet que l'échange de données entre l'administration du cadastre et l'administration de la fiscalité des entreprises et des revenus dans le but de contrôler certains citoyens entre dans l'exception au devoir d'information. Selon elle, « étant donné que la collecte indirecte de données par [l'administration de la fiscalité] a été réalisée en application de l'article 336 du CIR, la Commission considère que l'article 9, §2, alinéa 2, littera b) était d'application ; le SPF Finance était donc dispensé d'informer les contribuables concernés de la collecte indirecte de données par [l'administration de la fiscalité] auprès de [l'administration du cadastre] »[1260].

À notre sens, l'interprétation de la CPVP ne résiste pas à un examen sérieux. À l'heure de l'e-gouvernement et du principe de la collecte unique, la collecte indirecte des données des citoyens, effectuée « par ou en vertu d'une loi, d'un décret ou d'une ordonnance », a vocation à devenir la règle. L'exception au devoir d'information pourra donc être invoquée très régulièrement, au détriment de la transparence à l'égard des citoyens. Compte tenu de cette évolution, il importe particulièrement de veiller

[1259] Note de S. VERSCHUERE, « Projet de note méthodologique concernant la portée et l'application de l'article 9, §2, alinéas 2 et 3 de la LVP », disponible sur demande auprès de la Commission de la protection de la vie privée. Cette note a été approuvée en séance du 17 octobre 2007.

[1260] CPVP, avis n° 27/2007 relatif à l'échange de données à caractère personnel entre administrations fiscales – Vérification fiscale subséquente aux demandes de remboursement de la taxe sur les opérations boursières illégalement perçue suite à l'arrêt de la Cour de Justice des Communautés européennes du 15 juillet 2004, p. 6, n° 31.

à l'interprétation stricte des exceptions à la protection de la vie privée des citoyens et de ne pas les étendre d'une façon telle que les personnes concernées voient leur droit à l'information vidé de son sens.

Il serait par exemple judicieux de prévoir que l'exception prévue à l'article 9, §2, alinéa 2, b) de la loi du 8 décembre 1992 ne puisse être invoquée qu'en étant cumulée avec l'exception prévue à l'article 9, §2, alinéa 1, c'est-à-dire, dans les cas où il est établi avec certitude que les personnes concernées disposent déjà de toutes les informations relatives à la collecte indirecte en question.

II. L'obligation de déclaration

366.- Considérations générales. Tout traitement de données doit, en principe, être déclaré à la CPVP, qui enregistre les déclarations dans un registre accessible au public. Néanmoins, ici encore, ce principe est assorti d'exceptions bénéficiant à nombre d'administrations.

A. Le principe de l'obligation de déclaration

367.- La déclaration et le registre public. En principe, en vertu de l'article 17 de la loi du 8 décembre 1992, toute administration qui met en œuvre un traitement de données à caractère personnel doit, au préalable, le déclarer à la CPVP. Cette déclaration doit indiquer un certain nombre d'éléments relatifs au traitement, tels que les coordonnées de l'administration responsable du traitement, les catégories de données traitées, la ou les finalité(s) poursuivie(s), etc.[1261].

En vertu de l'article 18 de la loi du 8 décembre 1992, la déclaration de traitement communiquée par l'administration à la CPVP est enregistrée par cette dernière dans une base de données légalement dénommée le « registre des traitements automatisés de données à caractère personnel ». Ce registre est plus couramment appelé le « registre public », car il est accessible au public, notamment à partir du site internet de la CPVP.

> Sur la page d'accueil du site www.privacycommission.be, un onglet intitulé « registre public » permet de rechercher un traitement déclaré en introduisant l'intitulé du traitement, le nom du responsable de traitement ou les coordonnées de celui-ci.

[1261] Les mentions que doit contenir la déclaration sont énoncées à l'article 17, §§3 et 6 de la loi du 8 décembre 1992.

> Un autre onglet, intitulé « déclaration », permet au responsable du traitement d'introduire sa déclaration en ligne. Cela répond aux préoccupations du Groupe 29 qui a, à plusieurs reprises, encouragé les mécanismes de notification électronique pour alléger la tâche des responsables de traitement[1262].

368.- La raison d'être de la déclaration et du registre public. L'obligation de déclaration se justifie au regard de son utilité pour le citoyen, le responsable de traitement et la CPVP.

La déclaration et le registre public doivent permettre au *citoyen* de « trouver tous les éléments nécessaires à l'exercice de [ses] droits »[1263]. Il s'agit en effet d'une mesure de transparence grâce à laquelle les personnes concernées peuvent prendre connaissance des traitements existants, interroger éventuellement le responsable de traitement pour obtenir davantage de renseignements et réagir si des abus sont constatés. De manière plus générale, cela « devrait aussi permettre au public (via le contrôle de la presse par exemple) d'avoir une vue d'ensemble des utilisations de données à caractère personnel en Belgique »[1264].

Pour le *responsable de traitement*, elle constitue un moyen de le sensibiliser aux obligations qui s'imposent lors d'un traitement de données, et de vérifier le respect des conditions légales en cette matière[1265].

La *CPVP* y trouve les éléments nécessaires pour prendre connaissance des traitements existants. Elle peut ainsi exercer ses missions de contrôle et apprécier la suite à donner aux plaintes éventuelles qui lui sont adressées[1266].

369.- Les difficultés. Tels qu'organisés aujourd'hui, on peut se demander si la déclaration et le registre public atteignent leurs objectifs.

[1262] Groupe 29, Document de travail : la notification, 3 décembre 1997, p. 8 ; Id., Rapport du groupe de travail « Art. 29 » sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne, 18 janvier 2005, p. 24.

[1263] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. Parl.,* Ch. Repr., sess. 1990-1990, n° 10610/1, p. 22.

[1264] *Idem.*

[1265] Groupe 29, Rapport du groupe de travail « Art. 29 » sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne, *op. cit.,* p. 6.

[1266] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, *op. cit.,* n° 1610/1, p. 22.

En effet, en consultant le registre public, le citoyen peut éprouver des difficultés à prendre connaissance des traitements existants à son sujet, et être ainsi découragé dans sa démarche.

> Par exemple, l'identification des traitements nécessite que l'on encode le nom du responsable de traitement ou la dénomination du traitement. Cela suppose que le citoyen ait déjà connaissance de ceux-ci et y accède au cas par cas. Il ne peut donc effectuer une recherche à partir du domaine qui l'intéresse, ce qui serait le cas s'il avait la possibilité de retrouver, par exemple, « tous les échanges de données en matière fiscale ». Comment considérer alors que le registre public permet d'avoir une « vue d'ensemble » des traitements de données, comme cela a pourtant été affirmé pendant les travaux préparatoires de la loi du 8 décembre 1992 ou qu'il offre aux personnes concernées « un aperçu de l'utilisation concrète des données à caractère personnel », comme le soutient la CPVP [1267]?

Par ailleurs, le registre public ne donne qu'une vue parcellaire des collectes et échanges de données existant au sein du secteur public. Nombre de traitements ne sont pas déclarés, soit parce que l'obligation de déclaration n'est pas respectée, soit en raison de l'existence d'exceptions importantes qui seront analysées ci-après[1268].

> Il est par exemple piquant de constater que le seul traitement déclaré par l'ONSS est le placement d'une caméra de vidéosurveillance, alors que cette administration fait partie du réseau sectoriel de la sécurité social et est impliquée dans de nombreux transferts de données.
>
> Un récent projet de loi portant sur la modification de la loi du 8 décembre 1992 et sur lequel nous reviendrons ultérieurement[1269] atteste que « dans la pratique, il s'avère que de nombreuses personnes et entreprises ne respectent pas cette obligation de déclaration. En 2008, la CPVP a enregistré au total 4 133 déclarations, dont 3 681 pour de nouveaux traitements. On peut supposer que le nombre de traitements réels est largement supérieur. [...] On méconnaît ainsi [...] le premier objectif du législateur, [qui] était non pas de créer des formalités administratives supplémentaires, mais de sensibiliser les intéressés aux aspects liés à la protection de la vie privée et aux conséquences possibles. Dans les faits, il s'avère que l'effet éducatif et sensibilisateur de ces formalités est très limité chez les intéressés »[1270].

[1267] Rubrique « registre public » sur le site www.privacycommission.be

[1268] Voy. *infra,* n° 370.-

[1269] Voy. *infra,* n° 380.-

[1270] Proposition de loi du 26 mai 2011 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitement de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information, *Doc. Parl.,* Ch. Repr., sess. 2010-2011, n° 53-1509/001, p. 5.

En outre, la compréhension des éléments du registre public pose également problème.

> Nombre de déclarations reprennent des termes imprécis. Par exemple, l'Office de sécurité sociale d'Outre Mer a déclaré un traitement intitulé « recensement des personnes en situation de handicap ». La finalité énoncée se réduit à « service public ».
>
> Des difficultés langagières s'ajoutent encore, puisque les déclarations sont en français ou en néerlandais mais ne sont pas traduites.

Par ailleurs, la déclaration de tous les traitements peut s'apparenter à une tâche administrative lourde à gérer tant pour l'autorité responsable que pour la CPVP, si bien que même les spécialistes européens de la protection de la vie privée encouragent les États-membres à développer le régime des exceptions[1271].

Enfin, en pratique, l'attitude de la CPVP interroge également l'intérêt de la déclaration et du registre public. En effet, bien que nombre de traitements soient dispensés de déclaration comme cela est étudié ci-après, la CPVP reçoit encore trop de déclarations pour contrôler chacune d'elles. Elle ne réagit qu'aux violations les plus flagrantes, dénoncées par la presse ou qui émergent des plaintes de citoyens[1272].

B. Les exceptions à l'obligation de déclaration

370.- Les exceptions au bénéfice de l'administration. Des exceptions à l'obligation de déclaration peuvent être organisées par arrêté royal, moyennant le respect de certains conditions mentionnées à l'article 17, §8, alinéa 1er, de la loi du 8 décembre 1992.

> Cette disposition affirme qu'« après avis de la Commission de la protection de la vie privée le Roi peut exempter certaines catégories de la déclaration visée au présent article lorsque, compte tenu des données traitées, il n'y a manifestement pas de risque d'atteinte aux droits et libertés des personnes concernées et que sont précisées les finalités du traitement, les catégories de données traitées, les catégories de personnes concernées, les catégories de destinataires et la durée de conservation des données ».

[1271] Groupe 29, Rapport du groupe de travail « Art. 29 » sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne, *op. cit.,* pp. 23 et 24.

[1272] Entretien avec un membre de la Commission de la protection de la vie privée, le 21 avril 2010.

Ces exceptions sont organisées par l'arrêté royal du 13 février 2001[1273], parmi lesquelles certaines s'appliquent à de nombreuses administrations, comme le montrent les articles 60 à 62 de cet arrêté royal.

> *L'article 60* affirme qu'« à l'exception des paragraphes 4 et 8[1274] de la loi, l'article 17 n'est pas applicable aux traitements effectués par les communes, conformément à la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, conformément à la législation électorale, ainsi qu'aux dispositions légales relatives aux registres de l'état civil ».
>
> *L'article 61* dispose qu' « à l'exception des paragraphes 4 et 8, l'article 17 de la loi n'est pas applicable aux traitements de données à caractère personnel, effectués par des autorités administratives, si le traitement est soumis à des réglementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées ainsi que leur utilisation et leur obtention ».
>
> Enfin, selon *l'article 62*, « les dispositions de l'article 17 de la loi, à l'exception des §§ 4 et 8, ne sont pas applicables aux traitements de données à caractère personnel, gérés par les institutions de sécurité sociale visées aux articles 1er et 2, premier alinéa, 2°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale et visant à appliquer la sécurité sociale, à condition que, pour ce qui concerne ces traitements, ces institutions satisfassent aux dispositions de la loi précitée et à ces arrêtés d'exécution.
>
> La liste, visée à l'article 46, premier alinéa, 6°bis, de la loi du 15 janvier 1990 relative à l'institution et l'organisation d'une Banque-Carrefour de la sécurité sociale, est tenue à disposition de la Commission de la protection de la vie privée, conformément aux modalités, déterminées de commun accord, par ces deux instances. Sur base de cette liste, la Commission de la protection de la vie privée met à jour le registre public des traitements de données automatisés de données à caractère personnel visé à l'article 18 de la loi ».

371.- La raison d'être des exceptions. Le régime d'exception est fondé sur le constat qu'aujourd'hui, le nombre de traitements automatisés de données à caractère personnel est si élevé qu'il est « pratiquement exclu de soumettre l'ensemble de ces traitements à l'obligation

[1273] Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel précité.

[1274] Les paragraphes 4 et 8 de l'article 17 de la loi du 8 décembre 1992 prévoient respectivement le droit de la CPVP de demander des informations complémentaires dans le cadre de son pouvoir d'enquête et de contrôle, et le pouvoir du Roi d'exempter certains traitements de l'obligation de déclaration.

de déclaration »[1275]. D'une part, cela nuirait au travail de la CPVP, qui « devrait consacrer tous ses moyens et toute son énergie au traitement desdites déclarations, de sorte qu'il resterait peu de place pour accomplir des missions plus essentielles »[1276]. D'autre part, cela porterait également atteinte à l'information des personnes concernées car « il serait extrêmement difficile de distinguer, parmi les millions de déclarations, celles qui pourraient présenter un risque d'atteinte à la vie privée »[1277].

Partant de ce constat, l'idée s'est imposée d'organiser un « filtrage »[1278] des déclarations, en exemptant de cette obligation les traitements de données qui « ne présentent à l'évidence aucun risque d'atteinte à la vie privée des intéressés »[1279].

Nombre de traitements effectués par les administrations sont ainsi exemptés de déclarations, au motif qu'ils sont encadrés par des dispositions légales ou réglementaires. Pour cette raison, on doit considérer que « le risque d'atteinte à la vie privée est minimalisé par l'existence des prescriptions spécifiques »[1280].

372.- Des exceptions larges. Comme en atteste la lecture des articles 60 à 62 susmentionnés, les exceptions organisées au bénéfice de l'administration sont particulièrement larges. La section de législation du Conseil d'État abonde d'ailleurs en ce sens[1281]. Elle soutient que les exemptions ne peuvent valoir que dans l'hypothèse où la réglementation applicable aux administrations visées contient l'ensemble des informations imposées par l'article 17, §8, de la loi du 8 décembre 1992, c'est-à-dire les informations qui doivent être mentionnées dans la déclaration de traitement.

Ainsi, s'agissant de *l'article 60 visant les communes*, la section de législation du Conseil d'État invite l'auteur du texte « à vérifier si les lois

[1275] Rapport au Roi précédant l'arrêté royal n° 13 portant exemption conditionnelle de l'obligation de déclaration pour certaines catégories de traitements automatisés de données à caractère personnel qui ne présentent manifestement pas de risque d'atteinte à la vie privée, *M.B.*, 15 mars 1996, p. 5803. Notons que l'arrêté royal n° 13 précède l'arrêté royal du 13 février 2001 précité et a été remplacé par ce dernier.

[1276] *Idem.*

[1277] *Idem.*

[1278] *Idem.*

[1279] *Idem.*

[1280] Rapport au Roi précédant l'arrêté royal n° 13 portant exemption conditionnelle de l'obligation de déclaration pour certaines catégories de traitements automatisés de données à caractère personnel qui ne présentent manifestement pas de risque d'atteinte à la vie privée, *op. cit.*, p. 2804.

[1281] SLCE, avis n° 30.495/2 du 8 novembre 2000.

auxquelles il se réfère satisfont à l'ensemble des exigences énoncées par l'article 17, §8, alinéa 1er, de la loi du 8 décembre 1992 ».

En outre, la section de législation du Conseil d'État désapprouve particulièrement *l'article 61 applicable aux autorités administratives*. Elle soutient que « les termes trop généraux de cette exemption ne garantissent pas que toutes les conditions d'exemption, énoncées à l'article 17, § 8, alinéa 1er, de la loi du 8 décembre 1992, sont remplies. Or, dans l'esprit de la loi, il convient que chaque réglementation soit examinée concrètement au regard des exigences formulées par l'article 17 précité. La disposition en projet doit, dès lors, être omise ou, à tout le moins, fondamentalement revue, de manière à désigner, avec précision, les réglementations concernées qui remplissent les conditions légales ».

Malheureusement, les arguments de la section de législation du Conseil d'État n'ont pas été suivis. Le Rapport au Roi relatif à l'arrêté royal du 13 février 2001 apporte des explications à ce sujet.

Concernant *l'article 60* et les traitements de données au sein des communes, il est avancé qu' « il serait dénué de sens d'obliger toute les communes belges à déclarer leur population, étant donné que ce traitement est déjà soumis à une réglementation stricte. En outre, d'autres traitements évidents, au niveau communal, tels que les registres de l'état civil ou les listes électorales, ne doivent pas davantage être déclarés ». Par ailleurs, en réponse à la remarque de la section de législation du Conseil d'État, le Rapport au Roi souligne que les lois auxquelles se réfère l'article 60 sont suffisamment précises, étant donné qu'elles mentionnent les conditions auxquelles les données sont radiées ainsi que la durée de conservation des données.

Concernant *l'article 61*, le Rapport au Roi soutient que « quoique la remarque du Conseil d'État ne soit pas dénuée de fondement, elle n'en demeure pas moins impraticable : le présent arrêté ne peut dresser une liste des lois à venir et examiner dans quelle mesure elles répondront aux conditions énoncées par l'article 17, §8. Par contre, l'article 61 précise que l'exemption de déclaration n'est valable que pour les traitements dont un règlement particulier règle la finalité du traitement, la collecte des données, ainsi que les modalités ».

Quant à *l'article 62* qui dispense les institutions de sécurité sociales de déclarer les traitements effectués en vertu de la loi du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale, le Rapport au Roi soutient que cette exemption est justifiée par la tenue d'un registre auprès du Comité sectoriel de la sécurité sociale. Ce registre reprend, pour chaque traitement effectué par une institution de sécurité sociale, les données qui doivent figurer dans une déclaration traditionnelle,

conformément à l'article 17, §3. Il doit être tenu à la disposition de la CPVP.

373.- Critiques. En somme, le Rapport au Roi justifie l'existence des exemptions au motif que, dans les cas prévus par l'arrêté royal du 13 février 2001, les personnes concernées connaissent déjà les éléments énoncés à l'article 17, §8, de la loi du 8 décembre 1992, à savoir, la finalité du traitement, les catégories de données traitées, les catégories de personnes concernées, les catégories de destinataires et la durée de conservation des données. Cette connaissance émanerait soit de la réglementation suffisamment précise qui encadre l'action de l'administration, soit du registre tenu par le Comité sectoriel de la sécurité sociale s'agissant des traitements de données effectués par des institutions de sécurité sociale.

Or, on peut raisonnablement penser que les personnes concernées ont rarement connaissance de ces éléments. Bien souvent, lesdites normes sont imprécises. Par ailleurs, le registre en matière de sécurité sociale est également critiquable.

a) Des normes imprécises. Comme l'a démontré le premier titre de la recherche, la réglementation des traitements est, pour l'heure, rarement si précise. Bien souvent, les traitements de données à caractère personnel se fondent sur des lois générales qui attribuent les compétences des administrations dans des matières déterminées. Ces lois ne contiennent pas les éléments requis par l'article 17, §8, précité. On peut espérer qu'à l'avenir, la situation soit différente car le législateur tiendrait compte des impératifs de protection de la vie privée lors de la confection des lois, comme l'y incite la CPVP.

> Ainsi, par exemple, à l'occasion de la rédaction d'un décret communautaire organisant une base de données, la CPVP a conseillé au législateur d'indiquer notamment la finalité poursuivie et la liste des données collectées et traitées dans ce cadre, ajoutant qu' « un encadrement légal répondant aux qualités pré-décrites aura [...] pour conséquence d'exempter le responsable du traitement de l'obligation de déclaration auprès de la Commission [...] en application de l'article 61 de l'A.R. du 13 février 2001 »[1282].

[1282] CPVP, avis n° 30/2008 du 3 septembre 2008 relatif à la constitution d'une base de données centrale des lecteurs/abonnés des institutions de prêt, visés aux articles 23 et 47 de la loi du 30 juin 1994 relative au droit d'auteur, soumises à l'obligation de payement de la rémunération pour prêt public et relevant de la compétence de la Communauté française, p. 6, n° 14.

On ne pourrait pas non plus justifier l'exemption par l'existence d'une autorisation de comité sectoriel. Il s'agirait là d'une dérive dangereuse. Comme cela sera étudié dans le troisième titre de la recherche, les comités sectoriels sont chargés d'autoriser les traitements de données. À cette occasion, ils se prononcent sur la finalité du traitement, les données utilisées, etc. Leurs décisions sont accessibles en ligne. Néanmoins, on ne peut considérer que l'existence de ces autorisations suffit à prouver la connaissance qu'ont les personnes concernées des éléments énoncés à l'article 17, §8, de la loi du 8 décembre 1992. En effet, ces décisions sont extrêmement nombreuses et bien souvent techniques, fondées sur un jargon complexe. On ne pourrait raisonnablement soutenir que les citoyens ont connaissance de ces autorisations et en comprennent les éléments qui y sont repris. Pourtant, cette dérive est à craindre, à en croire certains avis de la CPVP

> Par exemple, la CPVP reprochait à un projet d'arrêté royal de ne pas mentionner les données transmises lors des communications organisées. Elle constate néanmoins que ces communications de données exigent une autorisation du Comité sectoriel de la sécurité sociale et de la santé et soutient qu' « une telle autorisation principielle détaille la communication autorisée ce qui entraîne par nature sa transparence »[1283].

b) Le registre en matière de sécurité sociale. En vertu de l'article 46, §1, 6° *bis,* de la loi du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale, les institutions de sécurité sociale doivent déclarer leurs traitements auprès du Comité sectoriel de la sécurité sociale et de la santé, qui enregistre celles-ci dans un registre, appelé aussi « cadastre des interconnexions »[1284]. Ce registre doit être tenu à la disposition de la CPVP.

Cela signifie que les déclarations de traitement des institutions de sécurité sociale ne figurent pas dans le registre public détenu par la CPVP. En outre, le registre en matière de sécurité sociale n'est pas accessible au public. Il est simplement « tenu à la disposition » de la CPVP.

On comprend difficilement comment, dans ces circonstances, on peut considérer que les personnes concernées ont connaissance des éléments cardinaux des traitements de leurs données, comme le prévoit l'article 17, §8, précité.

*

[1283] CPVP, avis n° 04/2009 du 14 janvier 2009 concernant l'échange de données entre l'OCSC et les organismes percepteurs de cotisations de sécurité sociale, p. 6, n° 23.

[1284] Pour de plus amples détails à ce sujet, voy. *infra,* n°s 392.- et s.

Conclusions

374.- Une exigence cardinale. Dès les premières réflexions entourant la protection de la vie privée à l'égard des traitements de données à caractère personnel, l'importance de l'exigence de transparence a été mise en exergue.

Cet impératif conditionne l'effectivité du droit à l'autodétermination informationnelle de chaque individu garanti par l'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution. Pour connaître les traitements opérés sur les données, pour vérifier l'exactitude des informations utilisées et éventuellement dénoncer les abus qui seraient commis dans l'administration, des voies d'accès doivent être creusées vers les coulisses de l'e-gouvernement.

La transparence des traitements de données à caractère personnel permet ainsi d'équilibrer les pouvoirs de l'administration et du citoyen et conforte le bon fonctionnement de la démocratie.

375.- Les forces de la transparence des traitements de données à caractère personnel. Pour satisfaire à l'objectif ambitieux de la transparence des traitements de données à caractère personnel, la directive 95/46 et la loi du 8 décembre 1992 offrent aux citoyens des moyens d'action intéressants, qui tiennent compte des particularités des technologies.

Ainsi, la publicité passive de l'administration comporte notamment le droit d'accéder à la logique qui sous-tend les décisions automatisées, ce qui s'avère utile à l'heure du déploiement des techniques de profilage. Par ailleurs, des outils facilitent concrètement l'exercice du droit d'accès. À cet égard, le répertoire des références de la Banque-Carrefour de la sécurité sociale permet au citoyen de situer ses données au sein du réseau sectoriel de la sécurité sociale, tandis que l'accès en ligne au Registre national offre à chacun un accès direct à ses données et aux informations relatives aux consultations de celles-ci.

Plus encore, le régime de protection des données accorde une attention particulière à la publicité active des traitements de données. L'utilisation des informations dans l'univers dématérialisé doit bénéficier d'une visibilité semblable à celle que l'on connaissait dans l'administration traditionnelle. Ainsi, une exigeante obligation d'information s'impose aux responsables de traitements, qui doivent avertir les personnes concernées des éléments majeurs concernant le traitement de leurs données. En outre, l'obligation de déclaration des traitements et l'enregistrement des déclarations dans le registre public sont censés offrir une vue d'ensemble des traitements de données en vigueur.

376.- Les limites de la transparence des traitements de données à caractère personnel. Malheureusement, à maints égards, les outils de transparence organisés par le régime de protection des données à caractère personnel sont déforcés dans le contexte de l'e-gouvernement.

D'une part, la mise en pratique de la loi du 8 décembre 1992 se heurte à des embûches. À cet égard, la procédure d'accès s'avère, paradoxalement, peu accessible pour un citoyen exerçant raisonnablement sa curiosité légitime. Par ailleurs, la mise en œuvre de l'obligation d'information et de l'obligation de déclaration aboutissent à communiquer aux personnes concernées des informations tantôt trop nombreuses, tantôt trop obscures.

D'autre part, la transparence des traitements de données à caractère personnel est assortie de nombreuses exceptions, bénéficiant singulièrement à l'administration. Ainsi notamment, les citoyens sont bien souvent privés de la publicité active des échanges de données entre les administrations, au motif que ces traitements sont organisés par ou en vertu d'une loi.

De telles limites apportées à la transparence des traitements de données à caractère personnel font craindre l'opacité grandissante de l'administration face à des citoyens de plus en plus transparents.

*

CHAPITRE III.
L'organisation d'un e-gouvernement transparent

Introduction

Les deux premiers chapitres situent l'e-gouvernement aux confins de la transparence administrative et de la transparence des traitements de données à caractère personnel. Ils ont souligné les forces et les faiblesses de ces règles dans l'e-gouvernement.

Fort de ces enseignements, le présent chapitre propose des solutions pour assurer la transparence de l'e-gouvernement. Elles passent par la mise en place de certains outils techniques, et l'adoption d'un cadre juridique nouveau. Elles sont justifiées par plusieurs impératifs.

*

Section 1. Des impératifs

377.- Considérations générales. Deux impératifs doivent être pris en compte au moment de définir les règles qui garantissent la transparence de l'e-gouvernement. Il y a lieu, d'une part, d'organiser la convergence de la complémentarité de la transparence administrative et de la transparence des traitements des données à caractère personnel. Il importe, d'autre part, d'actualiser ces règles en fonction des technologies existantes.

Le premier titre de la recherche a proposé la rédaction d'une loi-cadre relative à l'e-gouvernement[1285]. Il a alors été question d'y intégrer certaines exigences applicables à tous les traitements de données réalisés dans ce domaine. Cette loi-cadre pourrait être enrichie des règles de transparence applicables à l'e-gouvernement.

[1285] Voy. *supra,* n°s 206.- et s.

I. L'organisation de la convergence et de la complémentarité des règles

378.- Convergence. La transparence administrative et la transparence des traitements de données à caractère personnel convergent vers une visée commune, celle de la protection des libertés[1286]. Ce constat justifie qu'on envisage la transparence administrative et la transparence des traitements de données à caractère personnel comme les parties d'un tout[1287].

Ainsi qu'on l'a dit précédemment[1288], la transparence administrative s'inscrit dans le prolongement de la liberté d'expression, consacrée par l'article 10 de la CEDH, tandis que la transparence des traitements de données à caractère personnel, visée par l'article 8 de la CEDH, contribue à la protection de la vie privée des citoyens.

Ce faisant, ces règles favorisent l'exercice de la démocratie. Puisque la personne concernée est en mesure de savoir ce que l'administration détient de manière générale, et ce qu'elle possède à son sujet en particulier, elle peut participer au débat démocratique en pleine connaissance de cause et se trouve à même de contrôler l'action publique au travers de l'usage qui est fait des informations détenues par les institutions publiques. Forte d'une telle connaissance, il lui est loisible de dénoncer les abus éventuels.

a) L'arrêt Guerra. L'arrêt *Guerra*[1289], rendu par la Cour européenne des droits de l'homme, met en évidence la convergence entre la transparence administrative et la protection de la vie privée.

> Dans cette affaire, quarante italiennes résidant à un kilomètre d'une usine chimique à haut risque saisissent la Cour européenne des droits l'homme pour que soit condamné l'État italien. Elles reprochent à ce dernier de ne pas les avoir informées des dangers de cette usine ni des mesures à prendre en cas d'accident ou, en d'autres termes, de ne pas avoir assuré la publicité

[1286] Pour une analyse sur la manière de combiner, actuellement, l'application de la loi du 8 décembre 1992 et la loi du 11 avril 1994, voy. L. Moens, « Passieve openbaarheid van bestuur en privacybescherming », *in Het handvest van de sociaal verzekerde en bestuurlijke vernieuwing in de sociale zekerheid* (dir. J. Put), Brugge, die Keure, 1999, pp. 208 à 275 ; C. de Terwangne, « Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles : regards croisés sur deux voies d'accès à l'information », *in Transparence et droit à l'information*, Liège, collection *Formation Permanente CUP*, vol. 55, pp. 85 à 115.

[1287] Au moment d'organiser la transparence de l'e-gouvernement, il faudra donc cerner les points communs entre ces règles, de manière à en organiser l'application simultanée.

[1288] Voy. *supra,* n° 240.- et 325.-

[1289] Cour eur. D.H., *Guerra c. Italie,* 19 février 1998. Pour un commentaire cette décision au regard de la mission publique d'information, voy. C. de Terwangne, « La Cour européenne des droits de l'homme et le droit de recevoir des informations de la part des autorités publiques », *Amen. Env.,* 1998, pp. 265 à 270.

> active desdites informations. Les requérantes fondent leur argumentation sur l'article 10 et l'article 8 de la CEDH.

Dans son arrêt, la Cour européenne des droits de l'homme conclut qu'il n'y a pas eu de violation de l'article 10 de la CEDH, vraisemblablement pour des raisons propres à l'affaire[1290]. Par contre, elle juge que l'État italien devait assurer la communication active des informations relatives aux dangers de l'usine en vertu de l'article 8 de la CEDH. C'est la première fois qu'elle affirme un lien direct entre le droit fondamental à la vie privée et la communication active d'informations détenues par l'État.

> Selon la Cour, il s'agit d' « informations essentielles qui leur auraient permis d'évaluer les risques pouvant résulter pour elles et leurs proches du fait de continuer à résider sur le territoire de Manfredonia, une commune aussi exposée au danger en cas d'accident dans l'enceinte de l'usine »[1291]. Constatant le manquement des autorités italiennes de communiquer ces informations, elle conclut à la violation de l'article 8 CEDH en l'espèce.

Bien que cette affaire concerne des informations environnementales importantes pour la vie privée et la santé des individus, ce qui l'éloigne de notre sujet de recherche, l'arrêt *Guerra* confirme la convergence existant entre la transparence de l'administration et la protection de la vie privée des citoyens, et souligne l'importance d'envisager ces règles dans leur globalité. Cette convergence doit guider le législateur dans l'organisation de la transparence de l'e-gouvernement.

b) La solution québecquoise. La solution québecquoise donne corps à la convergence qui existe entre la transparence de l'administration et la transparence des traitements de données à caractère personnel. En effet, au Québec, les règles de transparence administrative et les règles de transparence des traitements de données à caractère personnel sont intégrées dans une même loi[1292].

Ce n'est pas là une simple question de forme. Le fait d'envisager cumulativement ces deux axes de la transparence emporte des conséquences sur la structure et le fonctionnement des organes de contrôles. Il n'y a pas, au Québec, un organe de contrôle dévolu à la transparence administrative distinct d'un autre organe dévolu à la protection des données à caractère personnel. La Commission d'accès à l'information du Québec traite des

---

[1290] Pour de plus amples précisions à ce sujet, voy. C. DE TERWANGNE, « La Cour européenne des droits de l'homme et le droit de recevoir des informations de la part des autorités publiques », *op. cit.,* pp. 265 à 267.

[1291] Cour eur. D.H, *Guerra c. Italie,* précité, §60.

[1292] La loi en question est la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L. R. Q., c. A-2.1.

questions d'accès aux documents administratifs et de protection des données à caractère personnel[1293].

Par ailleurs, cette solution est satisfaisante, d'après la Commission d'accès à l'information. Elle permet de traiter, de manière globale, les questions qui supposent l'application des deux corps de règles. Elle a également des conséquences culturelles positives, en favorisant la connaissance, par le public en général, des règles relatives aux traitements des données à caractère personnel. En effet, les règles relatives à la transparence administrative sont plus connues que les règles de protection des données à caractère personnel, car elles sont souvent invoquées par les journalistes qui souhaitent accéder à certains documents détenus par l'État. Le fait que les journalistes évoquent quotidiennement la « loi sur l'accès aux documents publics et sur la protection des renseignements personnels » rappelle aux québecquois que les renseignements personnels sont protégés[1294].

Bien que l'intégration, dans une seule loi, des règles de transparence administrative et de protection des données à caractère personnel paraisse judicieuse, nous ne la développons pas davantage dans le cadre de cette recherche. La mise en œuvre d'une telle solution en Belgique impliquerait tant de modifications importantes à maints égards qu'elle dépasse largement le cadre de cette recherche. Dès lors, dans les lignes qui suivent, nous nous concentrons sur les pistes de solutions qui nous paraissent être, pour l'heure, les plus réalistes[1295].

379.- Complémentarité. La transparence administrative et la transparence des traitements de données à caractère personnel s'enrichissent mutuellement. Malheureusement, cette complémentarité n'apparaît pas suffisamment dans l'arsenal normatif actuellement applicable à l'e-gouvernement. C'est pourquoi, les solutions nouvelles exposées dans la suite de la recherche visent à organiser concrètement cette complémentarité.

a) La transparence administrative améliore la transparence des traitements de données à caractère personnel. Puisque le citoyen peut en principe accéder à tout document permettant de comprendre la structure et le fonctionnement de l'administration, il est en mesure de savoir dans quelles bases de données seront enregistrées ses informations personnelles,

[1293] Art. 103 et s. de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. À propos de l'activité de la Commission d'accès à l'information du Québec, voy. http://www.cai.gouv.qc.ca/

[1294] Entretien avec la Directrice des affaires juridique à la Commission d'accès à l'information du Québec, Stéphanie Regnier et Cynthia Chassigneux, juristes à la Commission d'accès à l'information du Québec, Montréal, le 16 avril 2012.

[1295] Voy. *infra,* n°s 384.- et s.

ainsi que l'usage qui sera fait de celles-ci, et ce, avant que la collecte et le traitement de ces données aient lieu.

Cette connaissance *a priori* des traitements de données à caractère personnel complète utilement le travail du législateur qui, en vertu de l'article 22 de la Constitution, doit veiller à la prévisibilité de la loi organisant une ingérence dans la vie privée. De cette manière, le citoyen peut se fonder sur la loi et sur les voies d'accès organisées par la transparence administrative pour savoir ce qu'il adviendra de ses données une fois collectées par l'administration.

Par ailleurs, la loi sur la motivation formelle des actes administratifs peut également être très intéressante dans le cadre de l'e-gouvernement. La motivation des actes administratifs vise à permettre à l'administré de comprendre la décision qui le concerne. L'adaptation de cette loi à l'e-gouvernement pourrait s'avérer utile pour permettre au citoyen de comprendre les traitements de données effectués en amont d'une décision.

b) La transparence des données à caractère personnel affine la transparence administrative. La collecte et l'utilisation des données à caractère personnel forment aujourd'hui une part substantielle de l'action administrative. Dès lors, sans la transparence des traitements de données à caractère personnel, le citoyen n'aurait qu'une vue parcellaire de l'action publique. Sa compréhension de l'administration dans son ensemble serait tronquée. Grâce aux voies d'accès résultant de l'exigence de transparence des traitements de données à caractère personnel, le citoyen peut obtenir de nombreuses informations précises qui l'interpellent directement puisqu'il s'agit de ses propres données. En outre, cet accès est aisé, car il ne dépend que de la preuve de l'identité du demandeur.

Pourtant, à l'heure actuelle, l'enrichissement mutuel des deux régimes de transparence n'apparaît pas clairement car les voies d'accès issues de la transparence administrative et celles imposées par la transparence des traitements de données à caractère personnel sont organisées par des législations distinctes, et soumises à des procédures présentant chacune des particularités.

L'organisation de la transparence de l'e-gouvernement est donc l'occasion de cerner les points communs entre ces règles, de manière à en organiser l'application simultanée.

II. L'actualisation des règles

380.- Les raisons justifiant l'actualisation des règles. Il est impératif de simplifier l'exercice des droits d'accès organisés par la transparence administrative et la transparence des traitements de données à caractère

personnel. Leur complexité actuelle décourage le citoyen d'exercer ses droits d'accès dans l'e-gouvernement. Cette simplification pourrait se faire en exploitant les potentialités des technologies existantes. En somme, « il ne s'agit plus simplement d'assurer le droit à l'information du citoyen vis-à-vis de son administration mais, de manière plus volontariste, de transformer, grâce aux technologies, cette administration devenue transparente en un meilleur service aux citoyens »[1296].

Actuellement, certains outils technologiques sont déjà utilisés dans l'administration pour améliorer la transparence administrative et la transparence des traitements de données à caractère personnel. Malheureusement, ces techniques sont mises en place de manière éparse et restent limitées à certains domaines de l'administration.

> Par exemple, comme il en a déjà été fait état, une application informatique permet à la personne concernée de vérifier, par internet, les administrations qui ont consulté ses données à caractère personnel. Néanmoins, cette possibilité est limitée aux données contenues au Registre national, via l'application https://www.mijndossier.rrn.fgov.be

La loi du changement et le principe de la réciprocité des avantages convainquent d'étendre, à l'ensemble de l'administration, les outils informatiques utiles à la transparence et d'en encadrer l'usage de manière claire et cohérente.

A. La loi du changement

381.- Le besoin de nouvelles mesures de transparence. La loi du changement, dite aussi « loi de mutabilité » ou « loi de fonctionnement efficace »[1297] permet[1298] aux pouvoirs publics d'adapter rapidement les services publics aux évolutions des exigences de l'intérêt général, en modifiant les règles d'organisation et de fonctionnement des services

[1296] C. Lamouline et Y. Poullet, *Des autoroutes de l'information à la 'démocratie électronique'. De l'impact des technologies de l'information et de la communication sur nos libertés*, Bruxelles, Bruylant, 1997, p. 98.

[1297] Au sujet des différentes appellations, voy. J.-P. Markus, « Le principe da'adaptabilité : de la mutabilité au devoir d'adaptation des services publics au besoin des usagers », *R.F.D.A,* 2001, p. 589.

[1298] Pour l'heure, il n'est pas certain que la loi du changement suffise à elle seule pour contraindre les pouvois publics d'effectuer les changements nécessaires. À ce sujet, voy. B. Gors, « Le principe de mutabilité », *in Le service public. 2. Les 'lois' du service public »* (dir. H. Dumont, P. Jadoul, B. Lombaert, F. Tulkens et S. Van Drooghenbroeck), *op. cit.,* pp. 167 et 168.

publics, ainsi que les conditions dans lesquelles les prestations sont fournies aux administrés[1299].

> La Cour constitutionnelle rappelle cette exigence dans sa jurisprudence, en affirmant que « d'une manière générale, les pouvoirs publics doivent [...] pouvoir adapter leur politique aux exigences changeantes de l'intérêt général »[1300].

La Charte de l'utilisateur des services publics est plus exigeante car elle impose clairement aux services publics de recourir aux technologies pour s'adapter aux évolutions des besoins du public.

> Ainsi cette Charte affirme-t-elle que « par application de la loi de mutabilité, les services publics doivent s'efforcer de procurer un service adapté aux besoins des utilisateurs, comme aux techniques et moyens disponibles »[1301].

Dans l'e-gouvernement, les besoins du public en matière de transparence sont amplifiés. En effet, les données à caractère personnel sont aujourd'hui la matière première du fonctionnement de l'administration et même, le « pétrole du numérique »[1302]. Sans elles, les réseaux sectoriels, les plateformes d'échanges, les entrepôts de données, les sources authentiques de données ne peuvent fonctionner.

Il importe donc aujourd'hui d'organiser des voies de transparence réellement efficaces, qui permettent aux citoyens de connaître notamment les circuits d'informations, de corriger les erreurs éventuelles et de dénoncer les abus possibles. La loi du changement permet aux administrations d'adapter leurs services à ce besoin nouveau. Plus encore, la Charte

---

[1299] M.-A. Flamme, « Service public et puissance publique, mythes ou réalités ? » *in Miscellanea W.J. Ganshof Van Der Meersch,* T. III, Bruxelles, Bruylant, Paris, L.G.D.J., 1972, p. 484 ; M. Boes et L.- P. Suetens, *Administratief recht,* Leuven, Acco, 1994, p. 65 ; M. Herbiet et A.-L. Durviaux, *Droit public économique,* Bruxelles, La Charte, 2008, p. 35 ; P. Goffaux, *Dictionnaire élémentaires de droit administratif*, *op. cit.,* pp. 170 et 171 ; D. Renders et L. Vansnick, « La place des lois du service public dans la hiérarchie des normes », *in Le service public. 2. Les 'lois'du service public »* (H. Dumont, P. Jadoul, B. Lombaert, F. Tulkens et dir. S. Van Drooghenbroeck), Bruxelles, La Charte, 2009, pp. 36 et s. ; B. Gors, « Le principe de mutabilité », *in Le service public. 2. Les 'lois'du service public »* (dir. H. Dumont, P. Jadoul, B. Lombaert, F. Tulkens et S. Van Drooghenbroeck), *op. cit.,* pp. 106 et s.

[1300] Voy. not. C.C., arrêt n° 29/2005 du 9 février 2005, B. 10.2.

[1301] Charte de l'utilisateur des services publics du 4 décembre 1992, Partie I, Chapitre II, Section 2. « Par application de la loi de mutabilité, les services publics doivent s'efforcer de procurer un service adapté aux besoins des utilisateurs, comme aux techniques et moyens disponibles ».

[1302] I. Falque-Pierrotin et S. Rozenfeld, « Les données personnelles représentent le pétrole du numérique », *Expertises,* 2012, pp. 49 à 54.

d'utilisateur des services publics le leur impose, tout comme le principe de la réciprocité des avantages dont il est question ci-après.

Pour répondre à ce besoin de transparence, les moyens techniques nouveaux doivent être pleinement exploités. Des outils pertinents existent déjà. On pense notamment au répertoire de références, qui indique la localisation des données au sein d'un réseau sectoriel. On pense également au portail du Registre national qui permet une consultation directe des données et une indication des autorités ayant consulté ces données. Au nom de la loi du changement, ces outils doivent aujourd'hui être utilisés plus largement au sein de l'administration.

C'est pourquoi, par exemple, la logique du droit d'accès doit être dépassée. Elle a été conçue par rapport à une structure administrative en silos et imprégnée d'une conception « papier ». Elle se révèle inadaptée à un e-gouvernement structuré en réseaux. La publicité active doit dès lors être développée davantage, notamment en utilisant internet et les potentialités informatiques pour mettre à disposition de tout citoyen un outil lui permettant d'obtenir, sans attendre, une vision claire de la structure de l'administration, en général, et la localisation de ses données à caractère personnel, en particulier.

B. Le principe de la réciprocité des avantages

382.- Le principe. L'actualisation des règles de transparence se justifie également au regard du principe de la réciprocité des avantages, dont il a déjà été question précédemment[1303].

Ce principe veut que le bénéfice des technologies profite tant aux citoyens qu'à l'administration. Puisque l'administration utilise les technologies pour renforcer l'efficacité de son action, cette même technologie doit être organisée au bénéfice des citoyens, pour faciliter l'exercice de leurs droits. C'est l'idée que « *within a democracy, citizen should not be left as pedestrians when the authorities drive limousines* »[1304].

> Le principe de la réciprocité des avantages peut faire évoluer, par exemple, la procédure du droit d'accès. Tant la loi du 11 avril 1994 que la loi du 8 décembre 1992 prévoient que le droit d'accès s'exerce par un écrit et que l'identité du demandeur doit être justifiée, ce qui signifie qu'une copie de la carte d'identité électronique doit être fournie. En appliquant le principe de la réciprocité des avantages, on aboutit à soutenir qu'il faut actualiser ce droit

[1303] Voy. *supra*, n° 166.-

[1304] D.W. SCHARTUM, « Access to Government-Held Information : Challenges and Possibilities », *The Journal of Information Law and Technology*, 1998/1, §7.1.

d'accès et donner à chacun la possibilité de l'exercer par voie électronique, à l'aide d'un lecteur de carte d'identité électronique si la preuve de l'identité doit être fournie.

Autre exemple. La loi du 11 avril 1994 prévoit des obligations de publicité active à charge de l'administration. La loi du 8 décembre 1992 organise un registre public des traitements de données. En combinant ces règles et en les actualisant en application du principe de la réciprocité des avantages, on peut affirmer la nécessité de développer l'utilisation des cadastres d'interconnexions et de prévoir un accès en ligne à ceux-ci.

La section 2 qui suit montre qu'on peut faire évoluer d'autres règles de transparence par application du principe de réciprocité des avantages.

383.- Les justifications du principe. Quatre raisons au moins justifient l'application du principe de la réciprocité des avantages dans le contexte de l'e-gouvernement.

a) L'équilibre entre le citoyen et l'administration. La loi du 11 avril 1994 sur la publicité de l'administration et la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs, notamment, témoignent de l'équilibre que le législateur a veillé à instaurer entre le citoyen et l'administration dans le contexte de l'administration « papier ».

L'exposé des motifs de la loi du 11 avril 1994 confirme ces propos. Ainsi, le Ministre de l'Intérieur et de la Fonction publique a-t-il soutenu que « dans toute organisation politique, le citoyen doit occuper une position centrale et on ne peut accorder à aucune structure le droit ni le pouvoir de se substituer au citoyen, ni de le mettre dans une position d'inégalité et, par hypothèse, d'infériorité. Il va sans dire qu'un tel principe doit également s'appliquer à l'administration, à son organisation et à son fonctionnement »[1305].

La recherche de cet équilibre a également retenu l'attention du législateur lors de l'élaboration des règles de traitements de données à caractère personnel. C'est la raison pour laquelle la loi du 8 décembre 1992 organise notamment des voies d'accès aux données à caractère personnel.

Lors des discussions préparatoires à l'adoption de la loi du 8 décembre 1992, il a été affirmé que les règles relatives aux traitements de données à caractère personnel, et, notamment, les obligations de transparence, ont été conçues de manière à « assurer un équilibre entre les nécessités de la protection de la vie privée et celles d'une politique administrative, économique et sociale bien organisée. Les obligations imposées au [responsable du traitement] sont

[1305] Projet de loi relatif à la publicité de l'administration, Exposé des motifs, *op. cit.*, p. 4.

établies de façon à ce que les charges soient réduites sans porter atteinte aux droits des particuliers »[1306].

Dans l'e-gouvernement, les droits offerts aux citoyens ne suffisent plus, comme tels, à garantir cet équilibre, étant donné que la puissance administrative est renforcée par la technologie. C'est pourquoi, la technologie doit également renforcer les droits des citoyens, notamment en ce qui concerne la publicité de l'administration et la transparence des traitements de données qui les concernent[1307]. On peut ainsi affirmer que, dans l'e-gouvernement, l'autodétermination informationnelle ne peut être une réalité qu'à la condition que chaque individu puisse bénéficier des potentialités de l'informatique[1308].

La CPVP reprend ce principe dans sa jurisprudence, en insistant sur le maintien de l'équilibre entre le pouvoir de l'administration et les prérogatives du citoyen. « Les capacités d'investigation fiscale de l'État seront nettement renforcées du fait de la mise en place, au sein du SPF Finances, d'outils technologiques de pointe tel qu'un système intégré d'aide à la prise de décision comprenant des données à caractère personnel collectées en interne au sein des services du SPF Finances et en externe dans des bases de données externes publiques (DIV, Emploi,…) et privées (taux de consommation d'énergie). La Commission considère dès lors qu'il est effectivement indispensable qu'une réciprocité des avantages soit mise sur pied, conformément à ce qui est explicité dans l'exposé des motifs. À ce titre, vu les projets en cours, une

[1306] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel et proposition de loi relative à la protection de données personnelles concernant les personnes physiques dans les fichiers informatiques ou banques de données et à la création d'une commission nationale de l'informatique et des libertés, Rapport fait au nom de la Commission de la Justice par Mme Merckx-van Goey, *Doc. Parl.*, Ch. repr., session 1991-1992, n° 413/12, p. 6.

[1307] H. Burkert, « Data protection and Access to Data », *in From Data protection to Knowledge Machines* (P. Seipel éd.), Deventer, Boston, Kluwer Law and Taxation, 1990, pp. 49 et s. ; D.W. Schartum, « Access to Government-Held Information : Challenges and Possibilities », *The Journal of Information Law and Technology*, 1998/1, §4 ; C. de Terwangne, *Société de l'information et mission publique d'information*, *op. cit.*, pp. 300 et 301 ; Y. Poullet, « Pour une troisième génération de réglementation de protection des données », *in Défis du droit à la protection de la vie privée. Perspectives du droit européen et Nord-américain* (dir. M.V. Perez Asinari et P. Palazzi), Bruxelles, Bruylant, 2008, pp. 57 et 58. Voy. égal. CPVP, avis n° 01/2007, *op. cit.*, p. 15, n° 83.

[1308] Dans le même sens, T. Würtenberger et G. Sydow affirment que « l'autodétermination informationnelle dans la société de l'information existe précisément grâce à la possibilité pour les citoyens d'utiliser les potentialités de l'informatique, et n'implique que secondairement la défense des dangers qui les menacent ». (Voy. T. Würtenberger et G. Sydow, *op. cit.*, p. 366).

> augmentation du contenu du devoir d'information, telle que prévue à l'article 26 de l'avant-projet de loi est effectivement indispensable »[1309].

b) La ratio legis des normes organisant l'e-gouvernement. Les développements de l'e-gouvernement s'accompagnent généralement de justifications législatives vantant l'intérêt des technologies pour l'efficacité de l'administration, mais également l'allègement des formalités administratives imposées au citoyen.

> Par exemple, la nécessité de mettre en place la Banque-Carrefour de la sécurité sociale est justifiée par le fait que « des efforts exagérés sont demandés aux citoyens, aux assurés sociaux, aux employeurs lors de la communication aux organismes de sécurité sociale, des données nécessaires à l'établissement de leurs droits [...] La création de la Banque-Carrefour doit permettre de réduire pour les personnes physiques et morales intéressées, les charges ou obligations ». Et d'ajouter un argument pris du principe de la réciprocité des avantages, qui consiste à dire qu'« une rationalisation convenable de la collecte, de l'enregistrement et du traitement des données [...] s'impose d'autant plus que les technologies disponibles permettent de l'atteindre avec toutes les garanties souhaitables »[1310].

Il serait donc absurde de s'évertuer à simplifier de plus en plus de démarches administratives mais de ne pas reconnaître que le principe de réciprocité des avantages doit être appliqué aux démarches relatives à la transparence de l'administration pour simplifier celles-ci.

c) La ratio legis des normes organisant la transparence de l'administration. On a dit précédemment que les règles de transparence sont adoptées pour permettre au citoyen de comprendre son environnement administratif, participer à la vie démocratique en pleine connaissance de cause, et contrôler l'action des pouvoirs publics[1311]. La satisfaction de tels objectifs aujourd'hui impose de reconnaître l'application du principe de la réciprocité des avantages à l'e-gouvernement[1312].

De toute évidence, la version informatique d'un document, par exemple, est plus riche que sa version papier, puisqu'on peut notamment soumettre le document informatique à un outil de recherches par mots-clés, ce qui n'est pas possible avec une version papier. Dès lors, si l'administration dispose du document en version informatique, il serait

---

[1309] CPVP, avis n° 01/2007, *op. cit.*, p. 83.

[1310] Projet de loi relatif à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *Doc. Parl.*, Ch. Repr., sess. 1988-1989, n° 899/1, *Pasin,* 1990, I, p. 77.

[1311] *Voy. supra* 241.- et s. et n°s 325.- et s.

[1312] En ce sens, voy. C. de Terwangne, *Société de l'information et mission publique d'information*, *op. cit.*, pp. 298 et 299.

contraire à la raison d'être des règles de transparence de le communiquer au citoyen en version papier.

> Par exemple, les données des citoyens circulent au sein du réseau sectoriel de la sécurité sociale. Les administrations de ce réseau qui réclament des données les obtiennent rapidement et aisément, grâce à la Banque-Carrefour de la sécurité sociale. Celle-ci assure le transit des données grâce à des tables informatiques indiquant quel type de donnée se trouve où et qui peut accéder à quoi[1313].
>
> Comment une personne pourrait-elle connaître, comprendre et contrôler les traitements de données effectués dans ce réseau sectoriel si, lorsqu'elle demande d'obtenir une copie de la table « quoi-où » pour comprendre quel type de données se trouve dans quelle administration, on lui répond[1314] qu'elle doit reconstituer elle-même cette table à partir des autorisations de comités sectoriels qui sont pourtant extrêmement nombreuses et sont reprises, certes sur internet, mais sans autre classement que l'ordre chronologique ? Il faut au moins lui fournir la copie de la table des données disponibles (table « quoi-où ») idéalement en version informatique ou, au moins, en version papier.

d) Le financement des technologies par l'impôt. Un quatrième argument, lié au coût des technologies, convainc d'appliquer le principe de la réciprocité des avantages à l'e-gouvernement. En effet, dans la mesure où la mise en place des outils de traitements de données est financée par l'impôt, il est difficilement justifiable que le contribuable ne puisse bénéficier des avantages de ces outils qu'il a lui-même financés.

Henry H. Perrit affirme notamment que « value added information element pertaining to core missions or supporting internal agency functions, paid for with tax dollars, should presumptively be maid available for the public »[1315].

[1313] Voy. *supra*, n° 25.-

[1314] Voy. *supra*, n° 299.-

[1315] H. H. Perritt, *Public Information in the National Information Infrastructure,* Report to the Regulatory Information Service Center, General Services Administration, and to the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, 20 mai 1994, p. 3.

Section 2. Des solutions

384.- Objectif. Les impératifs qui viennent d'être décrits convainquent d'utiliser les outils technologiques pour faciliter davantage l'exercice, par les citoyens, des droits que leur octroient les règles de transparence.

Cet objectif pourrait être atteint en organisant un portail internet à partir duquel toute personne intéressée pourrait accéder à une vue d'ensemble de l'administration, au travers de sa structure et des documents qu'elle détient. Il faut également veiller à ce que la personne curieuse puisse prendre connaissance d'une vue individualisée de son dossier, qui divulgue les informations relatives au traitement de ses données par les autorités publiques.

> À nouveau, le Québec propose une solution intéressante dans la lignée de ces réflexions. Depuis le 29 novembre 2009, les québecquois peuvent accéder, en ligne, à des informations relatives principalement à la structure et au fonctionnement de l'administration en général, et utiles tant pour la transparence administrative que la transparence des traitements de données.
>
> Ainsi, l'article 4 du Règlement sur la diffusion de l'information et sur la protection des renseignements personnel[1316], pris en application de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[1317], impose aux organismes publics de diffuser sur leur site internet diverses informations d'intérêt général, parmi lesquelles figurent
>
> « 1° l'organigramme,
>
> [...]
>
> 3° le nom du responsable de l'accès aux documents et de la protection des renseignements personnels et les coordonnées permettant de communiquer avec lui ;
>
> [...]
>
> 5° l'inventaire de ses fichiers de renseignements personnels établi en vertu de l'article 76 de la Loi ».

Les développements qui suivent envisagent des solutions qui faciliteraient l'accès, par chacun, à une vue d'ensemble de l'administration et une vue individualisée du parcours que suivent les données personnelles au sein du secteur public.

[1316] Règlement sur la diffusion de l'information et sur la protection des renseignements personnel, c. A-2.1, r. 2.

[1317] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L. R. Q., c. A-2.1.

385.- Remarque générale : le droit d'accès électronique. La loi du 11 avril 1994 et la loi du 8 décembre 1992 organisent toutes deux un droit d'accès qui s'exerce par écrit[1318]. En outre, toute demande d'accès aux données à caractère personnel doit s'accompagner de la preuve de l'identité du demandeur, c'est-à-dire une copie de sa carte d'identité.

Dans l'e-gouvernement, de manière générale, le droit d'accès doit pouvoir être effectué en ligne, par internet. En effet, les échanges de données entre les administrations sont considérablement facilités par l'utilisation des technologies. Les contacts entre l'administration et les citoyens doivent l'être aussi[1319].

Une proposition de loi visant à modifier la loi du 8 décembre 1992[1320] s'inscrit dans le sens de cette préoccupation. Elle souligne l'importance de consacrer un « droit à la portabilité des données », c'est-à-dire, le droit de chacun de recevoir une copie électronique de ses données à caractère personnel.

L'article 2 de la proposition de loi dispose que « le droit de consultation donne lieu, en cas de traitement automatisé, à la communication de ces données sous une forme électronique compréhensible, efficace et conviviale. La possibilité d'accéder aux données de manière non numérique, si la personne concernée le souhaite, est maintenue ».

> L'ajout de cette précision législative qui viendrait compléter l'article 10 de la loi du 8 décembre 1992 est motivé comme suit : « l'obligation de communiquer les données à caractère personnel sous une forme intelligible, prévue dans la loi sur la protection de la vie privée, n'est actuellement pas toujours interprétée comme étant l'obligation de fournir une copie de ces données sous une forme électronique utilisable.
>
> En 1992, la Belgique a adapté sa législation relative à la protection de la vie privée en vue de prendre en compte les traitements automatisés. Le nombre de traitements automatisés et leur impact ont fortement augmenté depuis 1992. Maîtriser ses propres données à caractère personnel est plus que jamais une nécessité. Sous l'impulsion de l'internet à haut débit et des services web 2.0, de plus en plus de données sont chargées, traitées et stockées sur l'internet même. Des services web "dans les nuages" ont vu le jour pour le

[1318] Art. 5 de la loi du 11 avril 1994 ; art. 10, §1, de la loi du 8 décembre 1992. Voy. *supra,* n° 255.- et n°s 331.- et s.

[1319] Dans le même sens, voy. C. DE TERWANGNE, *Société de l'information et mission publique d'information, op. cit.*, pp. 297 et s.

[1320] Proposition de loi du 26 mai 2011 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitement de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information, *Doc. Parl.*, Ch. Repr., sess. 2010-2011, n° 53-1509/001.

> traitement de textes, de photos, de comptabilités, de signets, de coordonnées, … Tout citoyen doit pouvoir choisir en toute liberté de télécharger ses données : lorsqu'il souhaite réaliser un backup de ses données, les examiner plus en détail, changer de prestataire de services, … La transparence favorise la confiance du consommateur dans les nouvelles technologies. La portabilité des données stimule le caractère innovateur et concurrentiel du marché »[1321].

La proposition de règlement européen sur la protection des données[1322] consacre également un droit à la portabilité des données, qui permet à la personne concernée d'obtenir notamment « une copie des données faisant l'objet du traitement automatisé dans un format électronique structuré qui est couramment utilisé et qui permet la réutilisation de ces données »[1323].

Dans les lignes qui suivent, on encourage la création d'un portail internet à partir duquel la personne pourrait trouver les documents qu'elle recherche, sans même devoir adresser une demande d'accès à une personne en particulier. Si la justification de l'identité est requise, elle pourrait se faire en utilisant la carte d'identité électronique et un lecteur de cartes.

Néanmoins, il se pourrait que la personne ne trouve pas le document dont elle a besoin[1324]. Elle devrait alors pouvoir contacter l'administration par internet et effectuer sa demande d'accès en ligne. Cela suppose que les coordonnées de la personne de contact qui, au sein des institutions publiques, est chargée de répondre aux citoyens, apparaissent clairement sur le site de chaque institution.

386.- Remarque générale : les exceptions à la transparence. Comme il en a été question à plusieurs reprises, nombre d'exceptions actuellement en vigueur empêchent les citoyens de satisfaire pleinement leur curiosité légitime. À l'occasion de la redéfinition des obligations de transparence dans l'e-gouvernement, cette problématique doit être réévaluée.

Remarquons qu'avec la mise en ligne des documents administratifs, certaines exceptions perdent leur raison d'être. On pense à l'exception

---

[1321] *Ibid.*, p. 4.

[1322] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personne physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final.

[1323] Art. 18.1 de la proposition de règlement sur la protection des données.

[1324] En tout cas, la personne intéressée rencontrera cette difficulté avant que le portail internet dédié à la transparence soit mis en place.

relative au caractère abusif de la demande, organisée par la loi du 11 avril 1994. La mise en ligne des documents ainsi accessibles par tous facilite considérablement le travail de l'administration. On imagine mal une institution publique pouvoir soutenir que la publicité du document perturberait le service ou gênerait le fonctionnement de celui-ci.

En revanche, on ne peut pas remettre en cause le fait que les exceptions nécessaires à la pérennité de l'État doivent subsister. Celles-ci sont liées à la protection de la sécurité, de l'ordre public, et des intérêts économiques de l'État. Certaines de ces exceptions sont organisées par la loi du 11 avril 1994 sur la publicité de l'administration et d'autres le sont par la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs. Par contre ces exceptions ne sont pas prévues par le régime de protection des données à caractère personnel mais gagneraient à l'être afin, notamment, de ne pas mettre à néant certaines opérations de profilage.

Ces exceptions devraient être reprises dans la loi-cadre sur l'e-gouvernement à la condition d'être explicitement limitées. Ainsi faudrait-il affirmer que le principe est la publication des informations sur le portail internet. Si une exception peut être avancée, elle ne peut aboutir nécessairement à la confidentialité complète du document. Il y a lieu, en effet, d'envisager d'abord la divulgation partielle du document, dont on a enlevé les informations qui ne peuvent être divulguées. S'il est établi que le document doit rester secret dans sa totalité, son existence doit tout de même être mentionnée sur le portail et accompagnée de la justification, en fait et en droit, de la confidentialité imposée.

I. L'accès à une vue d'ensemble de l'administration

387.- Publicité active. Les obligations de publicité active organisées par la loi du 11 avril 1994 imposent à l'administration de fournir, d'initiative, « une information claire et objective sur l'action des autorités administratives fédérales »[1325]. De son côté, la loi du 8 décembre 1992 impose la mise en place d'un registre public, permettant de connaître les traitements de données qui ont été déclarés par les administrations.

Il faut à présent améliorer ces obligations de publicité active pour les adapter à l'e-gouvernement. À cette fin, il serait judicieux de permettre à chacun d'accéder aisément à un index des documents pertinents relatifs à l'action administrative en général, ainsi qu'à un panorama de la structure administrative et un cadastre des interconnexions.

[1325] Art. 2 de la loi du 11 avril 1994.

A. L'index des documents généraux pertinents

388.- Un outil de communication administrative informative. La recherche a déjà souligné la nécessité de développer la communication informative de l'administration, c'est-à-dire l'information portant sur les services et les activités de l'administration[1326].

> Par exemple, une enquête menée entre juin 2005 et octobre 2006 à la demande de Fedict atteste que « seul un internaute sur trois n'éprouve aucun problème dans la recherche d'informations publiques sur Internet. Ce n'est pas tant [...] la fiabilité des informations qui pose problème mais plutôt la facilité de trouver ces informations. Il apparaît en outre que les informations publiques disponibles sont souvent insuffisantes (et nécessitent d'être complétées à travers d'autres canaux d'information tels que le téléphone ou l'e-mail) et insuffisamment adaptées aux demandes ou aux situations personnelles spécifiques »[1327].

En particulier, on a mis en évidence l'existence, au sein des institutions œuvrant au fonctionnement de l'e-gouvernement, de rapports, d'études, d'analyses et l'intérêt que leur publication présenterait pour le public.

Rappelons qu'en créant récemment le portail http://data.gov.be, le Gouvernement fédéral a franchi une étape qui manifeste la volonté des pouvoirs publics d'ouvrir au public les ressources informationnelles détenues par les administrations. Il serait judicieux de prolonger ce mouvement récent d'ouverture en incitant le législateur à organiser la création d'un index exhaustif des documents permettant de comprendre la structure et le fonctionnement de l'e-gouvernement. Cet index devrait reprendre, pour chaque administration, la liste des documents existants et accessibles au public. Idéalement, ces documents devraient être disponibles en format informatique, de sorte que le citoyen n'ait qu'à cliquer sur un hyperlien pour y accéder. S'ils n'existent qu'en version papier, l'index devrait mentionner les données de contact de la personne pouvant fournir l'information recherchée.

389.- Des exemples à l'étranger. Certaines législations étrangères répondent à cette préoccupation et organisent des solutions intéressantes pouvant inspirer le législateur belge.

[1326] *Voy. supra*, n°s 309.- et s.

[1327] SPF FEDICT, Fed-eView Citizen. Étude longitudinale d'Internet et de l'e-government en Belgique. La parole au citoyen. Enquête réalisée par Indigov à la demande de Fedict, 2006, p. 18 disponible sur le site http://www.fedict.belgium.be/fr/binaries/Fed-eView%2520Citizen%2520Paper%25201.1_Final_FR_tcm166-9117_tcm461-127440.pdf

> Ainsi, aux États-Unis, le *Freedom of Information Act* présente deux particularités qui retiennent l'attention. D'une part, cette norme impose aux administrations de tenir un index de divers documents à disposition du public. Si les documents ne sont pas indexés, ils ne peuvent être invoqués à l'encontre d'un citoyen[1328]. D'autre part, chaque administration doit également tenir un index général reprenant l'indication des documents ayant déjà fait l'objet d'une demande de la part d'un administré et qui, compte tenu de leur nature ou de leur objet, sont susceptibles d'être demandés à nouveau[1329].
>
> Au Québec, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnel*s impose aux organismes publics de tenir une liste de classement de leurs documents, afin que ces derniers soient aisément identifiables[1330]. En outre, depuis le 29 novembre 2009[1331], les organismes publics sont tenus de publier, sur leur site internet, des documents tels que « 4° le plan de classification de ses documents exigé en vertu du deuxième alinéa de l'article 16 de la Loi ou, selon le cas, la liste de classement exigée par le premier alinéa de cet article ;
>
> [...]
>
> 7° les études, les rapports de recherches ou de statistiques, produits par l'organisme public ou pour son compte dont la diffusion présente un intérêt pour l'information du public ;
>
> […]
>
> 10° la description des services qu'il offre et des programmes qu'il met en œuvre ainsi que les formulaires qui s'y rattachent »[1332].

B. Le panorama de la structure administrative

390.- Un outil de communication administrative institutionnelle. Rappelons-le, la communication administrative institutionnelle vise la diffusion des informations « portant sur les services et les activités des institutions »[1333]. Pour le moment, chaque institution assure la publication des informations qui la concerne, ce qui ne permet pas d'avoir une vue d'ensemble de la structure de l'administration. Or, une telle vue

---

[1328] Section 552, (a)(2) du Freedom of Information Act.

[1329] Section 552, (a)(2)(E) du *Freedom of Information Act.*

[1330] Art. 16 de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, Lois refondues du Québec, chapitre A-2.1.

[1331] Art. 16.1 de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, Lois refondues du Québec, chapitre A-2.1.

[1332] Art. 4 du Règlement sur la diffusion de l'information et sur la protection des renseignements personnel précité.

[1333] C. DE TERWANGNE, *Société de l'information et mission publique d'information, op. cit.,* p. 383. Voy. *supra* n° 308.-

d'ensemble est importante dans l'e-gouvernement en réseaux pour comprendre l'environnement administratif dans lequel circulent les données à caractère personnel et ainsi satisfaire à la raison d'être des règles de transparence[1334].

Il convient donc que chacun puisse visualiser les réseaux sectoriels et les plateformes d'échanges d'informations, localiser les sources authentiques de données et les entrepôts de données. D'ailleurs, comme on l'a dit[1335], un tel effort de clarté contribue à « vulgariser par tous les vecteurs de communication adéquats les axes majeurs » de la politique des services publics, comme l'y invite la Charte de l'utilisateur des services publics[1336].

391.- Un panorama général. Une solution serait de créer un panorama général de la structure administrative offrant suffisamment d'informations sur les outils de traitements de données qui structurent l'administration, ainsi que les échanges de données mis en place.

Le panorama général devrait reprendre l'ensemble des réseaux sectoriels composant l'administration.

En outre, en cliquant sur le réseau sectoriel de son choix, le citoyen devrait voir apparaître la liste des administrations détenant une source authentique de données.

Enfin, en cliquant sur le nom de la source authentique, le type de données enregistrées par celle-ci devrait figurer sur l'écran.

Par ailleurs, certaines administrations utilisent un entrepôt de données commun. L'existence d'un tel outil de traitement devrait également apparaître sur le panorama général. En cliquant sur un lien, la liste des types de données traitées par cet outil devraient être accessibles.

C. Le cadastre des interconnexions

392.- Notion. Rappelons-le[1337], le développement de l'e-gouvernement se fonde sur le principe de la collecte unique des données, ce qui entraîne une multiplication des échanges de données entre les administrations.

Ces échanges de données doivent faire l'objet d'une publicité sur le portail internet dédié à l'e-gouvernement. Cela constituerait une mesure prolongeant, dans l'e-gouvernement, la volonté du législateur d'organiser

---

[1334] Voy. *supra,* n° 383.-

[1335] Voy. *supra,* n° 308.-

[1336] Chapitre 1er, 1., de la Charte de l'utilisateur des services publics du 4 décembre 1992.

[1337] Voy. *supra,* n° 10.-

la publicité active de l'administration, comme en atteste la loi du 11 avril 1994[1338], et de publier les traitements de données effectués par les administrations dans un registre public, accessible en ligne, comme le prévoit la loi du 8 décembre 1992[1339].

À cette fin, le cadastre des interconnexions est un outil particulièrement pertinent. Il peut être défini comme un registre qui répertorie les échanges de données effectués entre les administrations d'un même réseau sectoriel[1340].

La CPVP encourage l'utilisation de cet outil dans le contexte de l'e-gouvernement. Toutefois, elle n'a pas manqué de rappeler que la mise en place d'un cadastre des interconnexions ne peut dispenser le législateur d'adopter par ailleurs une loi qui encadre précisément les échanges de données.

> Ainsi affirme-t-elle qu' « un cadastre ne peut pas compenser un manque de qualité dans la base légale [...] [qui] doit être prioritaire. La transparence doit *a priori* être garantie par le législateur via une base légale de qualité. Le législateur doit déterminer les principes de base concernant qui peut échanger quoi pour quelle finalité. Le but [du cadastre] ne peut être de permettre l'échange de toutes les données à caractère personnel pour une finalité indéterminée par [...] des acteurs indéterminés sous prétexte que les interconnexions sont mentionnées par la suite dans un registre public. Ce serait la même chose si on n'attendait plus d'un portier qu'il vérifie si chaque visiteur remplit les conditions pour avoir accès mais qu'il se contente de demander à chacun de noter sa visite dans un registre public. La deuxième forme de contrôle est incontestablement beaucoup moins stricte »[1341].

393.- Consécrations légales actuelles. Actuellement, trois lois organisent la mise en place d'un cadastre d'interconnexions.

[1338] Art. 2, 1°, de la loi du 11 avril 1994. Voy. *supra,* n° 302.-

[1339] Art. 18 de la loi du 8 décembre 1992. Voy. *supra* n° 367.-

[1340] Au sujet du cadastre des interconnexions, voy. not. CPVP, avis n° 30/98 du 25 septembre 1998 relatif au registre national, p. 4 ; CPVP, avis n° 28/1999 du 8 septembre 1999 relatif à un avant-projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, p. 6 ; CPVP, avis n° 25/2000 du 10 juillet 2000 relatif au projet d'arrêté royal autorisant l'Intercommunale pour la gestion et la réalisation d'études techniques et économiques, en abrégé I.G.R.E.T.E.C., à utiliser le numéro d'identification du registre national des personnes physiques, p. 4, n° 2 ; CPVP, avis n° 19/2002 du 10 juin 2002 relatif à un projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et modifiant la loi d du 8 août 1983 organisant un Registre national des personnes physiques [...], p. 10, n° 18.

[1341] CPVP, avis n° 23/2008 du 11 juin 2008 relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules, p. 33, n° 108.

La loi du 8 août 1983 organisant un registre national des personnes physiques institue un cadastre qui reprend les connexions au registre national.

> L'article 8, §1, alinéa 4, de la loi du 8 août 1983 dispose que « les connexions au réseau découlant de l'utilisation du numéro d'identification du Registre national sont spécifiquement mentionnées dans la demande introduite en vue d'obtenir cette autorisation, afin de permettre au comité sectoriel de publier le cadastre des connexions au réseau. Toute modification des connexions au réseau découlant de l'utilisation du numéro d'identification du Registre national doit être soumise au préalable à l'approbation du comité sectoriel. [...] ».

La loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque carrefour de la sécurité sociale crée un cadastre qui répertorie les échanges de données entre institutions de sécurité sociale.

> L'article 46, §1, 6° *bis* de la loi du 15 janvier 1990 dispose que « [...] la section sécurité sociale du comité sectoriel de la sécurité sociale et de la santé est chargée, en vue de la protection de la vie privée, des tâches suivantes :
>
> [...]
>
> 6*bis*° tenir à jour un relevé qui contient, d'une part, pour ce qui concerne chaque traitement automatisé de données à caractère personnel effectué par une institution de sécurité sociale en vue de l'application de la sécurité sociale, au moins les données visées à l'article 17, § 3, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, telles que communiquées ou validées par l'institution de sécurité sociale concernée, et, d'autre part, les communications autorisées en vertu de l'article 15, ainsi que celles dont la section sécurité sociale du comité sectoriel de la sécurité sociale et de la santé doit être informée conformément au même article 15 ; le Roi fixe les modalités selon lesquelles toute personne intéressée peut consulter cette liste auprès de la Banque carrefour ».

La mise en place d'un troisième cadastre est également consacrée par la *loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules*. Il reprend les échanges de données entre les administrations reliées à la Banque-Carrefour des véhicules. Toutefois, son existence effective dépend d'un arrêté royal qui n'a pas encore été adopté.

> L'article 20 de cette loi prévoit que « les échanges entre les services, via le numéro d'identification unique du véhicule, de données à caractère personnel autres que celles reprises dans la Banque-Carrefour sont préalablement communiqués au service de gestion qui répertorie ces données d'interconnexion dans un cadastre, lequel peut être consulté par toute personne

intéressée. Le Roi détermine, après avis du comité sectoriel, les modalités de consultation et de communication des données figurant dans le cadastre des interconnexions ».

394.- Les difficultés. Les deux cadastres d'interconnexions qui, pour l'heure, fonctionnent de manière effective – à savoir, le cadastre du Registre national et celui de la Banque-Carrefour de la sécurité sociale – semblent davantage faciliter le travail de contrôle des comités sectoriels, qu'assurer la transparence des échanges de données à l'égard des citoyens.

En effet, d'une part, les échanges de données qui ont déjà été autorisés par le comité sectoriel compétent, ou qui ne doivent pas l'être, ne figurent pas dans le cadastre des interconnexions. Ces cadastres sont donc incomplets.

> S'agissant du cadastre du Registre national, la loi organise une exception importante à l'obligation d'enregistrer les traitements de données dans le cadastre. Elle affirme, en effet, que les « connexions au réseau » et les « transmissions de données » du Registre national ne sont pas soumises à cette obligation lorsque « une autorisation est accordée par un comité sectoriel créé au sein de la Commission de la protection de la vie privée »[1342].
>
> Quant à la loi du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale, elle soumet à l'obligation d'un enregistrement dans le cadastre des interconnexions « les communications autorisées en vertu de l'article 15, ainsi que celle dont la section sécurité sociale du comité sectoriel de la sécurité sociale et de la santé doit être informée ». Certaines communications ne répondent à aucune de ces deux hypothèses, en raison des exceptions qu'organise ce même article 15 de la loi du 15 janvier 1990. Plus encore, la pratique restreint encore davantage l'intérêt de ce cadastre puisque la Banque-Carrefour de la sécurité sociale considère que ce cadastre se réduit à la « liste des autorisations accordées par le Comité sectoriel de la sécurité sociale et de la santé »[1343].

D'autre part, aucune voie particulière n'a été mise en place pour faciliter l'accès du citoyen à ces registres. Ce dernier ne peut donc obtenir copie du cadastre qu'en utilisant la voie d'accès traditionnelle organisée par la loi du 11 avril 1994 relative à la publicité de l'administration. On peut donc difficilement soutenir que les cadastres des interconnexions visent à informer les citoyens des échanges de données dans l'administration.

[1342] Art. 8, §1, al. 5, de la loi du 8 août 1983.

[1343] Courriel de l'adviseur de la Banque-Carrefour de la sécurité sociale du 1er août 2011 en réponse à notre demande d'accès au cadastre des interconnexions.

> Concrètement, même en se fondant sur la loi du 11 avril 1994, un citoyen souhaitant obtenir une copie du cadastre des interconnexions entre institutions de sécurité sociale risque d'être insatisfait en constatant que la Banque-Carrefour de la sécurité sociale estime qu'elle « satisfait à cette obligation grâce à son site web sur lequel elle publie, dès que possible, les autorisations qui ont été accordées par le Comité sectoriel »[1344]. Pour le dire autrement, le « cadastre » se résume à l'accumulation des décisions du comité sectoriel sur le site internet de la Banque-Carrefour de la sécurité sociale, ce qui n'offre évidemment pas une vision claire des échanges de données entre institutions de sécurité sociale. Il faudrait, pour cela, lire toutes les autorisations du comité sectoriel et dresser soi-même le tableau identifiant les institutions et les données impliquées dans un échange.

395.- Les solutions. Il semblerait judicieux de veiller à ce que le cadastre des interconnexions soit une réelle mesure de transparence au bénéfice des citoyens. Cette conception devrait aboutir à structurer clairement le contenu de cet outil et à le rendre aisément accessible. Ce faisant, les personnes concernées pourraient prendre connaissance aisément des échanges de données entre administrations et, à partir de là, dénoncer éventuellement les abus commis.

En particulier, la loi-cadre sur l'e-gouvernement devrait déterminer le responsable du cadastre et prévoir des solutions pour améliorer l'accessibilité et la clarté de cet outil.

a) Le responsable du cadastre. Le cadastre des interconnexions devrait contenir la référence de l'ensemble des traitements de données effectués au sein du réseau sectoriel qui sont soumis à l'obligation de publicité. Dans cette perspective, il faudrait confier la tenue du cadastre des interconnexions à la plateforme d'échanges d'informations. En effet, dans le premier titre de la recherche, il a été proposé de transmettre à la plateforme d'échanges d'informations une copie de l'entente de partage en vue d'effectuer l'acheminement des données[1345]. À partir de ces demandes, la plateforme d'échanges d'informations pourrait créer et mettre à jour le cadastre des interconnexions du réseau sectoriel.

> En ce sens, la CPVP s'est récemment montrée défavorable à la désignation d'un comité sectoriel pour la tenue du cadastre des interconnexions de la Banque-Carrefour des véhicules. Elle estime que « toutes les interconnexions [...] ne sont pas soumises à une autorisation préalable du comité sectoriel ou à l'avis de la Commission [...]. Les organes de contrôle n'ont donc normalement pas la moindre connaissance de ces interconnexions qu'ils sont censés

[1344] *Idem.*

[1345] Voy. *supra,* n° 223.-

> contrôler ». Elle conseille de désigner le service de gestion de cette Banque-Carrefour, « étant donné qu'il est actif dans la matière et que son *core business* consisterait justement à gérer et à développer de tels flux de données »[1346].

b) L'accessibilité et la clarté du cadastre. Le cadastre des interconnexions devrait être accessible en ligne, dans le panorama général du portail internet. Etant donné qu'il doit exister un cadastre d'interconnexions par réseau sectoriel, le panorama devrait faire figurer le cadastre aux côtés du réseau sectoriel concerné.

> L'article 20 de loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules semble accorder un souci particulier à l'accessibilité du cadastre en affirmant que le cadastre des interconnexions « peut être consulté par toute personne intéressée ».

Dès lors que le cadastre des interconnexions doit permettre la transparence des échanges de données, il importe d'être attentif à la clarté de son contenu et de veiller à sa compréhension par le public. En effet, rappelons que l'article 10, §1, b) de la loi du 8 décembre 1992 impose que la communication des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données, soit effectuée « de manière intelligible ». Une telle obligation n'est pas respectée lorsque cette communication se réduit à la mise en ligne d'une liste d'échanges de données, qui est structurée à partir de la seule date de son effectivité, comme s'en contente actuellement le Comité sectoriel de la sécurité sociale et de la santé.

Un travail de classement rigoureux devrait donc être réalisé à partir des échanges de données mis en place. Ainsi, un tableau pourra être créé, duquel se dégageraient des catégories de données échangées, en fonction des demandeurs, des finalités, des types de données et des bases légales fondant le traitement.

II. L'accès à une vue individualisée de l'administration

396.- Des outils pour localiser les données. D'une part, la loi du 11 avril 1994 permet à chacun, en principe, de prendre connaissance des documents administratifs qui l'intéressent. D'autre part, la loi du 8 décembre 1992 impose à tout responsable de traitement de respecter certaines obligations d'information, en indiquant à la personne concernée

[1346] CPVP, avis n° 23/2008 précité, p. 33, n° 109.

la finalité des données collectées et les catégories de destinataires de ces informations, notamment.

Ces règles de transparence doivent être combinées et actualisées, pour être adaptées à l'e-gouvernement. Il faut ainsi que chacun puisse prendre connaissance aisément de la localisation de ses données au sein de l'administration, c'est-à-dire savoir dans quels réseaux sectoriels se trouvent ses données et, au sein de ces réseaux, dans quelles sources authentiques se situent-elles.

A. Le répertoire des références

397.- Des réseaux sectoriels et des sources authentiques multiples. Le premier titre de la recherche[1347] a montré l'intérêt, dans l'e-gouvernement en réseaux, de regrouper les administrations au sein de réseaux sectoriels dédiés chacun à un « événement de vie » particulier, à l'image du réseau sectoriel de la sécurité sociale. En outre, au sein de chaque réseau sectoriel, les données seraient disséminées entre des sources authentiques distinctes.

La multiplication des réseaux sectoriels et des sources authentiques de données risque de complexifier la localisation des données à caractère personnel au sein de l'administration. La personne concernée ne sachant pas nécessairement au sein de quel réseau se situent ses données, elle identifiera plus difficilement la source authentique à consulter pour accéder à celles-ci.

Une solution serait donc de créer un répertoire de références des réseaux et un répertoire de références des sources authentiques de données.

398.- Le répertoire des références des réseaux. Un répertoire des références des réseaux serait un document reprenant la liste des réseaux sectoriels au sein desquels circulent les données de la personne concernée. La personne pourrait l'obtenir en se connectant au portail internet dédié à la transparence de l'e-gouvernement, et en s'identifiant à l'aide de sa carte d'identité électronique. De cette manière, la personne serait en mesure de savoir que ses données se trouvent dans tels réseaux sectoriels mais non dans tels autres.

399.- Le répertoire des références des sources authentiques de données. Au sein d'un réseau sectoriel, les données d'un citoyen sont dispersées entre plusieurs sources authentiques de données. Toute personne

[1347] Voy. *supra,* n°s 134.- et s.

souhaitant prendre connaissance de ces données doit donc pouvoir disposer d'une liste énumérant les sources authentiques contenant des informations à son sujet[1348].

Dès lors, on pourrait prévoir le mécanisme suivant : une fois qu'il obtient le répertoire des références des réseaux sectoriels, le citoyen est en mesure de situer les réseaux détenant des informations à son sujet. Ensuite, en cliquant sur le nom d'un de ces réseaux, l'administré accède à la liste des sources authentiques contenant des données à son sujet. Cette liste est dénommée « le répertoire des références des sources authentiques de données du réseau » concerné. Enfin, en cliquant sur le nom de la source authentique qui l'intéresse, il peut consulter directement les données qui le concernent et vérifier leur exactitude.

B. L'*audit trail*

400.- La transparence du parcours des données. Pour comprendre pleinement comment l'administration traite ses données, le citoyen ne doit pas seulement connaître la localisation de celles-ci au sein des réseaux sectoriels et des sources authentiques de données. Encore faut-il qu'il ait connaissance du parcours suivi par ses informations entre les administrations qui les utilisent.

Les règles de transparence le justifient. On a vu qu'en imposant la motivation formelle des actes administratifs, la loi du 29 juillet 1991 organise le droit de chacun de comprendre le raisonnement qui sous-tend les décisions de l'administration. Dans l'e-gouvernement, cela suppose que le citoyen ait connaissance des traitements de données ayant permis à l'administration de prendre sa décision[1349].

Par ailleurs, la loi du 8 décembre 1992 affirme, en son article 12*bis*, que la personne soumise à une décision automatisée a le droit d'accéder aux éléments lui permettant de comprendre la logique qui sous-tend pareille décision[1350]. En outre, et plus encore, en vertu de l'article 10 de la loi du 8 décembre 1992, toute personne a le droit d'obtenir du responsable du traitement des indications sur les traitements de données effectués, parmi lesquelles figurent la finalité du traitement, l'origine des données et les destinataires de celles-ci[1351]. Dans l'e-gouvernement, le

[1348] En ce sens, N. Vandezande, D. De Cock, J. Dumortier, « ID-FIX: IDentification and Federal Inter-administration eXchange – eindrapport », Belspo, 2010, p. 32.

[1349] Voy. *supra,* n° 318.-

[1350] Voy. *supra,* n° 333.-

[1351] Voy. *supra,* n°s 328.- et s.

respect de telles exigences suppose que l'administration, responsable du traitement, fournisse un certain nombre d'informations « accessoires » relatives aux données « de base ». Ainsi l'administration doit-elle être en mesure de fournir à chaque personne des indications sur l'origine des données, la consultation de celles-ci, les transferts effectués à destination de qui et à quelles fins.

Pour satisfaire à cet objectif, la création d'un *audit trail* s'avère pertinente.

§1. La définition de l'*audit trail*

401.- La définition. Un *audit trail,* dit aussi *audit log,* se défini comme « un fichier qui contient toutes les données significatives qui fournissent une preuve qu'une transaction ou un événement spécifique s'est déroulé à un moment précis »[1352].

Pour le dire autrement, ce fichier contient les informations relatives aux traitements des données qui ont été effectués au sein de l'administration. Ces informations sont appelées « données de traçage », et sont les informations « accessoires » relatives aux données « de base ». Elles permettent à la personne concernée de savoir quelle institution a utilisé ses données, à quel moment, d'où provenaient lesdites informations, à quel destinataire elles ont été fournies ensuite et pourquoi.

Chaque échange de données entre les administrations est ainsi considéré comme le maillon d'une chaîne de traitements. L'ensemble de ces échanges mis bout à bout constitue un processus « *end to end* »[1353]. *L'audit trail* permet de rassembler ces maillons et de formaliser concrètement, de manière visible et compréhensible, le processus de traitements en chaîne. De cette manière, la personne concernée obtient une vue d'ensemble du parcours de ses données au sein de l'administration.

402.- Un outil de transparence et de contrôle. L'*audit trail* répond au souci d'assurer la transparence du parcours des données de chaque citoyen, en permettant à chaque administration de fournir à toute

[1352] Fedict, *Audit trail, une question de confiance. Analyse du contexte et des besoins de l'audit trail chez Fedict* (auteur : Olivier Schneider), Décembre 2007, p. 23. Dans le même sens, voy. Contrôleur européen à la protection des données, Avis sur la notification d'un contrôle préalable reçue du Délégué à la protection des données de la Commission européenne à propos du dossier « SYSPER 2 : évaluation professionnelle – REC », 15 décembre 2005, p. 8.

[1353] *Idem.*

personne concernée les informations nécessaires au sujet de l'utilisation de ses données[1354].

Par là même, *l'audit trail* est un outil de contrôle[1355]. Grâce aux indications relatives à l'utilisation des données, chaque personne est en mesure de vérifier la *légalité* des traitements opérés et d'identifier les usages suspects de celles-ci.

Les *erreurs* affectant les données peuvent également être plus facilement identifiées, tout comme la source de ces erreurs. Ce faisant, l'administration responsable des données erronées peut réagir efficacement.

Enfin, la *responsabilité* de chaque acteur intervenant dans la chaîne de traitements est encouragée, du fait de l'existence d'une possibilité de contrôle.

§2. Les données de traçage et la protection de la vie privée

403.- Considérations générales. L'enregistrement des données de traçage en vue de constituer un *audit trail* génère deux questions particulièrement intéressantes au regard de la protection de la vie privée. Il s'agit de savoir, d'une part, si le nom du fonctionnaire qui accède aux données doit être enregistré parmi les données de traçage et si la personne concernée peut connaître cette identité. D'autre part, on s'interroge sur la durée de conservation des données de traçage.

404.- L'identification de l'agent qui traite les données. On ne pourrait se contenter d'enregistrer seulement le nom de l'administration à partir de laquelle les traitements de données ont été effectués. Les données d'identification de l'agent qui traite les données doivent être enregistrées par l'administration au sein de laquelle il travaille et faire partie des données de traçage. C'est, en effet, la condition nécessaire pour rendre possible le contrôle des actes des fonctionnaires et sanctionner les abus éventuels dans l'usage des données[1356]. En d'autres termes, la protection réelle et effective des données à caractère personnel des citoyens suppose que le fonctionnaire ayant traité les données puisse être connu[1357].

[1354] Voy. *infra* n° 400.-

[1355] À ce sujet, voy. *infra,* n°s 401.- et s.

[1356] Voy. *infra,* Titre III.

[1357] En ce sens, C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données a caractère personnel », note sous C.J.U.E., 7 mai 2009, *College van burgemeester en wethouders van Rottredam c. m.e.e. Rijkeboer*, aff.C-553/07, *R.D.T.I.,* 2011, p. 76.

Dans son arrêt *I c. Finlande*, du 17 juillet 2008, la Cour européenne des droits de l'homme met en évidence l'importance de pouvoir identifier l'agent – et non seulement le service – ayant consulté les données[1358].

> Dans cette affaire, une infirmière, atteinte du virus HIV, est soignée dans l'hôpital au sein duquel elle travaille. Elle soupçonne des collègues d'avoir consulté son dossier et cherche à connaître l'identité précise de ceux-ci. Cela s'avère impossible en raison du fait, notamment, que l'hôpital en question ne conserve que l'identification des services accédant aux dossiers des patients, et non l'identification des personnes effectuant la consultation. La Cour européenne des droits de l'homme affirme qu'en l'espèce, l'article 8 de la Convention européenne des droits de l'homme est violé car, non seulement, l'accès aux dossiers médicaux n'est pas limité aux seules personnes qui interviennent dans le traitement du patient, mais, en outre, l'identification des personnes accédant aux dossiers n'est pas enregistrée.

Est-ce pour autant que le nom de ce fonctionnaire doit apparaître dans l'*audit trail* de la personne qui souhaite simplement connaître le parcours de ses données au sein de l'administration en se connectant au portail internet ? Nous ne le pensons pas.

Rappelons-le, cette question s'est posée il y a peu au sujet des données de consultation du Registre national, que toute personne intéressée peut visualiser en se connectant sur le site https://mondossier.rrn.fgov.be/. La CPVP a fait application de l'exigence de proportionnalité qui s'applique aux traitements de données. Elle a ainsi estimé que la mention du nom du fonctionnaire est disproportionnée au regard de l'objectif de transparence car « le citoyen ne peut tirer aucune conclusion quant au motif et à la régularité d'une consultation sur la seule base du nom du fonctionnaire ayant effectué celle-ci »[1359].

C'est pourquoi, l'*audit trail* devrait faire apparaître le seul nom de l'institution qui a enregistré telle donnée, a transféré telle autre, etc. Grâce aux données de contact des administrations qui devraient être aisément accessibles sur le portail dédié à la transparence de l'e-gouvernement[1360], le citoyen pourrait interroger ladite institution en vue d'obtenir davantage d'explications sur un traitement de données qui lui paraît suspect. Selon nous, il serait préférable, au regard de l'exigence de proportionnalité des

---

[1358] À ce sujet, voy. C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données a caractère personnel », *op. cit.*, pp. 76 et 81.

[1359] CPVP, avis n° 12/2009 précité, p. 7. Dans le même sens, voy. CPVP, recommandation n° 03/2010 du 9 juin 2010 relative à l'application des « *circles of trust* » (cercles de confiance) et à l'obligation de transparence concernant les consultations des informations du Registre national, p. 4, n° 11.

[1360] Voy. *supra,* n° 388.-

données, que l'identité du fonctionnaire ayant commis un usage abusif des données ne soit communiquée à la personne concernée que dans l'hypothèse où une action en responsabilité contre celui-ci est envisagée. En effet, dans ce cas, l'identité de l'agent doit être mentionnée dans l'acte de citation et il est donc nécessaire qu'elle soit connue de la personne souhaitant intenter l'action judiciaire.

405.- La durée de conservation des données de traçage. La question se pose également de savoir durant combien de temps ces données de traçage doivent être conservées.

La Cour de justice de l'Union européenne a récemment été saisie d'une question préjudicielle à ce sujet[1361].

> Dans cette affaire, un citoyen néerlandais, Monsieur Rijkeboer, introduit une demande d'accès auprès de sa commune, pour connaître l'identité des personnes et le contenu des informations communiquées au cours des deux années précédant sa demande. La commune répond favorablement à sa demande mais ne peut lui fournir que les informations remontant à un an avant sa demande, les autres ayant été automatiquement effacées. Monsieur Rijkeboer intente une action en justice contre la commune. La décision rendue en première instance est attaquée en appel. La juridiction d'appel interroge la Cour de justice de l'Union européenne en lui demandant, en substance, si le délai de conservation d'un an qu'applique la commune, est suffisant au regard du droit d'accès aux données à caractère personnel consacré à l'article 12 de la directive 95/46[1362].

Comme l'y invite la Cour, la fixation du délai de conservation des données de traçage doit tenir compte des exigences de finalité et de proportionnalité dont il a été longuement question dans le premier titre de la recherche[1363].

D'un côté, la *finalité* de l'enregistrement des données de traçage guide la détermination du délai. La Cour de justice de l'Union européenne met en évidence que ce délai doit être suffisamment long pour permettre à la personne concernée d'exercer les droits qui lui sont octroyés par la directive, à savoir, le droit d'obtenir la rectification ou l'effacement des

---

[1361] C.J.U.E., 7 mai 2009, *College van burgemeester en wethouders van Rottredam c. m.e.e. Rijkeboer*, aff.C-553/07. Pour un commentaire de cette decision, voy. C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données a caractère personnel », *op. cit.,* pp. 76 et 81 ; F. KAUFF-GAZIN, « Protection des données à caractère personnel », *in Europe,* juillet 2009, p. 15.

[1362] § 29 de l'arrêt. Rappelons que l'article 12 de la directive 95/46 correspond à l'article 10 de la loi du 8 décembre 1992.

[1363] Voy. *supra* n^{os}112.- et s.

données, le droit de s'opposer à un traitement, et le droit d'effectuer des recours juridictionnels en cas d'usage abusif de ses données[1364].

D'un autre côté, le délai de conservation des données de traçage ne doit pas être trop long, de manière à respecter l'exigence de *proportionnalité* des traitements de données. Il faut, en effet, veiller à ce que le délai de conservation n'impose pas une charge trop lourde au responsable du traitement, chargé de stocker ces données de traçage.

Enfin, certains paramètres peuvent aider à fixer le délai de conservation des données de traçage, tels que le délai pour introduire un recours et la durée de conservation des données de base[1365].

> Dans l'affaire soumise à la Cour de justice de l'Union européenne, le délai de conservation des données de traçage était d'un an, alors que les données de base étaient conservées bien plus longtemps. La Cour estime que ce délai « ne constitue pas un juste équilibre des intérêts et obligations en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement »[1366].

Pour le reste, et bien que ce ne soit pas une tâche aisée, le législateur doit apprécier, au cas par cas, la durée de conservation des données de traçage. S'agissant des données de traçage des informations enregistrées dans les sources authentiques de données de l'administration, il serait judicieux de se référer au délai durant lequel un recours en responsabilité extracontractuelle peut être intenté contre le fonctionnaire qui aurait utilisé abusivement les données. Cela signifie que les données de traçage devraient être conservées au moins 5 ans[1367].

[1364] §§ 51, 52 et 57 de l'arrêt.

[1365] § 63 de l'arrêt.

[1366] § 66 de l'arrêt.

[1367] Art. 2262*bis* du Code civil. Cette disposition affirme que « toute action en réparation d'un dommage fondée sur une responsabilité extra-contractuelle se prescrit par cinq ans à partir du jour qui suit celui où la personne lésée a eu connaissance du dommage ou de son aggravation et de l'identité de la personne responsable ». En l'occurrence, il nous semble peu envisageable de faire courir le délai de 5 ans à partir du moment où la personne aurait connaissance de l'usage abusif de ses données. En pratique, cela semble difficilement gérable pour l'administration responsable du traitement, qui devrait garder les données en attendant de savoir si, un jour, la personne concernée aurait connaissance du traitement illégal. Dès lors, et pour autant que la personne concernée ait aisément accès aux données de traçage relatives à ses informations personnelles, un délai de 5 ans à compter de la date du traitement de données et de son accessibilité via le portail internet, nous semble un délai raisonnable pour permettre à la personne concernée d'exercer ses droits, sans surcharger inutilement l'administration.

Ainsi, grâce à la connaissance des données de traçage, qui sont les accessoires des données de base, la personne concernée serait en mesure de garder effectivement la maîtrise de ses données personnelles et de voir protégé son droit à l'autodétermination informationnelle dans ses relations avec l'administration.

*

Conclusions

Dans ce chapitre, nous avons mis en évidence la convergence et la complémentarité de la transparence administrative et de la transparence des traitements de données à caractère personnel. Ces règles sont toutes nécessaires pour garantir la transparence de l'e-gouvernement.

Néanmoins, telles qu'elles sont rédigées actuellement, ces normes ne sont pas suffisantes pour mettre en lumière l'action de l'administration dans son contexte nouveau. En effet, l'e-gouvernement amplifie le besoin de transparence du public et rend nécessaire une actualisation de la législation. La loi du changement et le principe de la réciprocité des avantages justifient des solutions nouvelles, fondées sur un usage franc et généralisé des technologies, qui bénéficie tant à l'administration qu'aux citoyens.

Partant des points de convergence entre la transparence administrative et la transparence des traitements de données à caractère personnel, nous avons souligné l'intérêt de permettre à chacun d'accéder, d'une part, à une vue d'ensemble de la structure et des documents de l'administration et, d'autre part, au parcours suivi par ses données. Nous avons également montré que l'utilisation des technologies au bénéfice des citoyens permet de satisfaire ce besoin plus ample de transparence, en créant un portail internet dédié à la transparence et en utilisant des outils particuliers tels que le cadastre des interconnexions, le répertoire des références et l'*audit trail*. Ces solutions s'inscrivent dans la volonté du législateur d'assurer la transparence de l'administration mais paraissent mieux adaptées à l'e-gouvernement que les règles actuelles car elles offrent aux citoyens une transparence élargie de l'administration et des voies d'accès plus aisées aux informations qu'elle détient.

*

Conclusions du Titre II

Les règles de transparence administrative et les règles de transparence des traitements de données à caractère personnel guident aujourd'hui le citoyen avide de comprendre une administration longtemps perçue comme une forteresse entourée de secret.

Ces puits de lumières sont fondamentaux dans notre État de droit et, en particulier, dans l'e-gouvernement, car ils permettent au citoyen d'exercer une prise directe sur le fonctionnement de l'administration. Les règles de transparence contribuent dès lors au maintien d'un équilibre entre l'administration et le citoyen. Ainsi, en organisant l'accès aux documents administratifs et en obligeant les autorités administratives à motiver leurs décisions, la transparence administrative offre à chacun la possibilité d'être éclairé sur les politiques publiques et de participer au débat démocratique en pleine connaissance de cause. En cela, elle s'inscrit dans le prolongement de l'article 10 de la Convention européenne des droits de l'homme qui consacre la liberté d'expression et celle de recevoir des informations. Par ailleurs, la transparence des traitements de données à caractère personnel contraint l'administration de révéler, à la personne concernée, les informations qu'elle détient à son sujet et l'usage qu'elle en fait. Forte d'une telle connaissance, l'intéressé a conscience de ces traitements et il lui est loisible de dénoncer les abus éventuels. L'autodétermination informationnelle de chaque individu, protégée par l'article 8 de la Convention européenne des droits de l'homme, est ainsi confortée.

Néanmoins, au contact des technologies, ces règles révèlent des faiblesses si bien que l'objectif de transparence qu'elles poursuivent est menacé par l'e-gouvernement. En particulier, on a souligné notamment les difficultés d'exercer, dans une administration informatisée et en réseaux, des voies d'accès définies il y a plusieurs années, par rapport à une « administration papier » structurée alors en silos. Quant aux règles de protection des données, nous avons constaté que, même si elles ont été créées pour contrer les dangers de l'informatique, leur application à l'administration génère des problèmes et des frustrations.

Ces difficultés peuvent être résolues en admettant que les technologies, qui pour l'heure renforcent considérablement l'action de l'administration, doivent également bénéficier à chaque personne exerçant ses droits en matière de transparence. Le troisième chapitre a dès lors proposé des solutions fondées sur la mise en place d'outils nouveaux qui permettent au citoyen d'accéder, depuis son ordinateur, aux informations relatives à l'administration en général et aux traitements de ses données en particulier.

* * *

Titre III. Le contrôle de l'e-gouvernement

Introduction

Pour assurer l'effectivité des règles sur lesquelles ils se fondent, le droit administratif et le régime juridique de la protection des données à caractère personnel organisent des mécanismes de contrôle qui s'appliquent à l'administration en général et à l'e-gouvernement en particulier.

Confrontés au contexte de l'e-gouvernement, ces contrôles révèlent leurs forces et leurs faiblesses, auxquelles sont consacrés les deux premiers chapitres.

Finalement, dans le troisième chapitre, nous montrons que le renforcement du statut et des pouvoirs de la Commission de la protection de la vie privée[1368] permettrait d'améliorer substantiellement le contrôle de l'e-gouvernement.

* * *

[1368] Ci-après, « CPVP ».

CHAPITRE I.
L'e-gouvernement et le contrôle organisé par le droit administratif

406.- Introduction. Soumise aux exigences de légalité et de spécialité consacrées par le droit administratif[1369], l'administration est tenue de respecter les normes qui encadrent son action, parmi lesquelles figurent les règles de protection de la vie privée et des données à caractère personnel. Plusieurs formes de contrôle sont mises en place pour y veiller.

Ces contrôles sont qualifiés de « généraux » dans la mesure où ils ne sont pas propres aux questions de protection des données[1370].

En première ligne, il revient au ministre, qui exerce un contrôle hiérarchique sur les administrations, ainsi qu'à l'autorité de tutelle qui contrôle les autorités décentralisées[1371], de garantir le respect de ces règles. Le ministre et l'autorité de tutelle doivent notamment s'assurer que les éventuelles illégalités sont sanctionnées, à défaut de quoi, un sentiment d'impunité s'installerait dans ce domaine.

> Par exemple, le ministre doit veiller à ce que les agents ne cèdent pas à la tentation d'accéder aux bases de données à des fins privées, notamment pour satisfaire leur curiosité ou celle de leurs connaissances. De tels agissements sont illégaux. Leur auteur peut se voir infliger une peine disciplinaire, conformément à l'arrêté royal du 2 octobre 1937 portant le statut des agents de l'État (partie X – Régime disciplinaire).
>
> La gravité de la peine dépend de plusieurs facteurs, tels que l'utilisation des données à des fins privées ou pour des tiers, le fait que l'agent commet une illégalité pour la première fois ou non, etc.

Néanmoins, les règles de protection de la vie privée et des données à caractère personnel étant bien souvent floues et méconnues, il peut être judicieux que les ministres et les autorités de tutelle édictent des circulaires portant sur l'interprétation de ce régime juridique, de manière à prévenir les difficultés.

[1369] Voy. *supra*, Titre I.

[1370] C'est là une différence fondamentale avec le contrôle de la CPVP, qui sera étudié dans le chapitre 2.

[1371] Par exemple la Banque-Carrefour de la sécurité sociale est soumise au contrôle de tutelle du Ministre de la sécurité sociale.

> Par exemple, constatant que de nombreuses communes s'interrogent sur l'utilisation qu'elles peuvent faire des registres de la population et des étrangers, le ministre flamand des Affaires administratives, qui exerce la tutelle générale des communes, a émis des directives précises à ce sujet par une circulaire ministérielle du 1er juillet 2011[1372].

Au-delà du contrôle hiérarchique et du contrôle de tutelle qui ne soulèvent pas de questions particulières dans l'e-gouvernement[1373], l'administration est soumise à un contrôle juridique et à un contrôle politique exercés par des institutions diverses. Ces contrôles retiennent l'attention dans le présent chapitre.

Puisque ces institutions contrôlent l'administration en général, elles sont amenées à se prononcer sur l'e-gouvernement en particulier. D'emblée, on constate que ces contrôles traditionnels sont nécessaires dans le contexte de l'e-gouvernement. Ils offrent des voies d'action qui ne sont pas organisées par le régime juridique de la protection des données à caractère personnel. Inversement, les règles de protection des données nourrissent voire enrichissent ces contrôles traditionnels, en offrant des arguments nouveaux aux institutions chargées de veiller au bon fonctionnement de l'administration. De cette manière, le contrôle juridique et le contrôle politique s'immiscent aujourd'hui dans ce qui relevait, hier, du pouvoir discrétionnaire de l'administration et échappait à tout contrôle.

> On pense, notamment, à la mise en place d'une base de données par l'administration. Comme l'a montré le Titre I de la recherche, avant l'adoption du régime de la protection des données, la création d'un fichier relevait du pouvoir discrétionnaire de l'administration. Aujourd'hui, la mise en place d'une base de données doit être fondée sur une base légale et est soumise aux exigences de finalité, de proportionnalité, etc.

*

Section 1. Les contrôles juridiques

407.- Considérations générales. Les contrôles juridiques organisés par le droit administratif encadrent l'e-gouvernement. Ils sont exercés, d'une part, par des autorités non juridictionnelles – les autorités médiatrices et les autorités consultatives – et, d'autre part, par des autorités

[1372] Circulaire BB 2011/2 du 1er juillet 2011, Consultation des registres de population à des fins de gestion interne, *M.B.,* 26 juillet 2011.

[1373] Nous n'approfondissons donc pas ces contrôles dans notre recherche.

juridictionnelles – la Cour constitutionnelle, le Conseil d'État et les cours et tribunaux –. Certains aboutissent à une sanction contraignante, tandis que d'autres prennent la forme d'avis et de recommandations.

I. Le contrôle par les autorités non juridictionnelles

408.- Les autorités non juridictionnelles. L'e-gouvernement est soumis à l'examen d'autorités médiatrices et d'autorités consultatives.

A. Les autorités médiatrices

409.- Remarque préalable. Comme l'illustrent les développements qui suivent, le médiateur veille non seulement à la correcte application par l'administration des normes légales et réglementaires, mais il évalue également l'action administrative au regard de sources non formelles du droit que sont les principes de bonne administration[1374] et de bonne gouvernance[1375], ainsi que le principe d'équité[1376].

Comme l'affirme Pierre-Yves Monette, « au-delà du contrôle de légalité exercé par le juge, au-delà du contrôle de l'excès de pouvoir assuré par le juge administratif, l'ombudsman est également le contrôleur de la bonne administration, de la bonne gouvernance et celui de l'administration équitable »[1377]. Le médiateur peut « recommander l'adoption de solutions qui s'écartent de la lettre de la loi, lorsque l'application stricte de celle-ci, inéluctable en raison de la compétence liée de l'administration, aboutirait

[1374] Il s'agit, par exemple, du principe de gestion contentieuse (dit aussi « principe de prudence » ou « devoir de minutie »), du principe de la motivation des actes administratifs, du principe de l'information active et passive, du principe de proportionnalité, … À ce sujet, voy. not. J.-F. Neven et D. De Roy, « Principes de bonne administration et responsabilité de l'O.N.S.S. », *in La sécurité sociale des travailleurs salariés. Assujettissement, cotisations et sanctions* (dir. J.-F. Neven et S. Gilson), Bruxelles, Larcier, 2010, pp. 507 à 564 ; J. Jaumotte, « Les principes généraux du droit administratif à travers la jurisprudence administrative », *in Le Conseil d'État de Belgique, Cinquante ans après sa création (1946-1996)* (dir. B. Blero), Bruxelles, Bruylant, 1999, pp. 593-696. Voy. également *supra,* n°s 165.- et s.

[1375] Il s'agit notamment du principe du respect des valeurs démocratiques, du principe du respect des droits de l'homme et des libertés fondamentales, du principe de rigueur financière, du principe de moralité, du principe d'utilisation saine des ressources publiques, etc. Pour de plus amples détails à ce sujet, voy. P.-Y. Monette, « Du contrôle de légalité au contrôle de l'équité : une analyse du contrôle exercé par l'ombudsman parlementaire sur l'action de l'administration », *R.B.D.C.,* 2001, p. 22.

[1376] M. Verdussen, « Le médiateur parlementaire : données comparatives », *in Le médiateur,* Bruxelles, Bruylant, 1995, pp. 30 et 31 ; P.-Y. Monette, *op. cit.*, p. 5.

[1377] . P.-Y. Monette, *op. cit.*, p. 5.

dans les circonstances particulières de l'espèce, à créer une injustice flagrante que l'auteur de la loi aurait lui-même désapprouvée s'il avait eu connaissance desdites circonstances »[1378].

Les recommandations du médiateur touchant aux aspects de l'e-gouvernement sont le plus souvent fondées sur une norme contraignante ou sur un principe de bonne administration susceptible d'être rendu contraignant par la jurisprudence[1379]. C'est la raison pour laquelle on les étudie dans la partie consacrée au contrôle juridique de l'e-gouvernement.

§1. La présentation et le rôle du Médiateur

410.- La loi du 22 mars 1995 instaurant un Médiateur fédéral[1380]. La loi du 22 mars 1995 institue deux médiateurs au niveau fédéral, un néerlandophone et un francophone[1381].

Les communautés et les régions disposent également d'un médiateur, dont le statut et la fonction, organisés par décret, s'apparentent largement à celui du médiateur fédéral[1382]. C'est la raison pour laquelle la présente recherche se concentre sur le Médiateur fédéral.

Le rôle du Médiateur est double. Il est un conciliateur entre le citoyen et l'administration. Il est aussi un contrôleur de l'administration[1383].

411.- Un conciliateur et un contrôleur. Toute personne insatisfaite du fonctionnement ou d'un acte d'une autorité administrative peut

---

[1378] S. Van Drooghenbroeck, « L'équité et la Constitution. À propos de l'avis du Conseil d'État du 20 décembre 2000 sur une proposition de loi modifiant l'article 14 de la loi du 22 mars 1995 instaurant des médiateurs fédéraux », *C.D.P.K.*, 2001, p. 360.

[1379] Au sujet du caractère contraignant de ces principes, voy. P.-Y. Monette, *op. cit.*, pp. 18 à 21.

[1380] *M.B.*, 7 avril 1995.

[1381] Bien qu'ils soient deux médiateurs, nous parlerons « du Médiateur » dans les lignes qui suivent et ce, pour la facilité de la lecture.

[1382] Voy., pour la Communauté française et la Région wallonne, le décret du 31 mars 2011 portant assentiment à l'accord de coopération conclu le 3 février 2011 entre la Communauté française et la Région wallonne portant création d'un service de médiation commun à la Communauté française et à la Région wallonne, *M.B.*, 15 septembre 2011, p. 59873 ; pour la Communauté flamande, le décret du 7 juillet 1998 instaurant le service de médiation flamand, *M.B.*, 25 août 1998, p. 27221 ; pour la Communauté germanophone, le décret du 26 mai 2009 instituant la fonction de médiateur pour la Communauté germanophone, *M.B.*, 7 octobre 2009.

[1383] M. Verdussen, « Le médiateur parlementaire : données comparatives », *in Le médiateur*, Bruxelles, Bruylant, 1995, p. 24 ; H. Wuyts, « De ombudsman in perspectief », *TBP*, 1999, p. 416 ; P.-Y. Monette, *op. cit.*, p. 4.

introduire une réclamation auprès du Médiateur[1384]. Ce dernier tente alors de concilier les points de vue pour trouver une solution au différend qui oppose l'administré et l'administration.

Le Médiateur contrôle l'administration. À l'occasion de l'examen d'une réclamation, ou en investiguant auprès des services administratifs à la demande de la Chambre des représentants[1385], il peut être amené à constater un dysfonctionnement de l'administration, qui se manifesterait au travers de décisions illégales ou de procédures inéquitables par exemple.

412.- Des moyens d'action. Pour accomplir son rôle de conciliateur et de contrôleur, le Médiateur dispose de pouvoirs d'instruction, d'injonction et de dénonciation.

> La loi du 22 mars 1995 permet au Médiateur de « fixer des délais impératifs de réponse aux agents ou services », de « faire toute constatation sur place, se faire communiquer tues les documents et renseignements » qu'il estime nécessaires[1386]. Le médiateur dispose également d'un pouvoir de dénonciation au procureur du Roi, si, dans l'exercice de ses fonctions, il découvre un fait qui peut constituer un crime ou un délit.[1387]

À l'issue de sa mission, le Médiateur peut adresser à l'administration toute recommandation qu'il estime utile. Par ailleurs, il est tenu chaque année de faire rapport de ses activités à la Chambre, et peut à cette occasion lui adresser des recommandations également.

§2. Le Médiateur et l'e-gouvernement

413.- Les questions d'e-gouvernement. Naturellement, au gré du déploiement de l'e-gouvernement, le Médiateur est amené à connaître de réclamations portant sur des échanges de données entre administrations, sur des erreurs affectant les données utilisées, etc.

Ce phénomène génère des questions relatives à l'application de la loi du 8 décembre 1992. Il amène également le Médiateur à chercher des solutions aptes à répondre aux enjeux de l'e-gouvernement.

1384 Art. 8 de la loi du 22 mars 1995 précitée.
1385 Art. 1, 2°, de la loi du 22 mars 1995 précitée.
1386 *Ibid.,* art. 11.
1387 *Ibid.,* art. 12.

414.- Le Médiateur, l'e-gouvernement et la loi du 8 décembre 1992. Le Médiateur peut-il connaître de réclamations portant sur des traitements de données illégaux effectués par une administration ?

La loi prévoit que lorsque la réclamation concerne une autorité administrative « qui dispose de son propre médiateur en vertu d'une réglementation légale »[1388], le Médiateur est tenu de la transmettre à celui-ci. Cette règle est interprétée largement puisque toute instance de gestion des plaintes, externe à l'administration, est assimilée au « médiateur » visé par l'article 9 de la loi du 22 mars 1995[1389].

C'est pourquoi, une réclamation portant sur un traitement de données illégal sera transmise à la CPVP[1390] qui, comme il en sera question dans le deuxième chapitre de cette recherche, peut être saisie de toute plainte ayant « trait à sa mission de protection de la vie privée à l'égard des traitements de données à caractère personnel ou d'autres missions qui lui sont confiées par la loi »[1391].

Le Médiateur fédéral a déjà transmis plusieurs réclamations à la CPVP[1392]. Dans sa tâche de gestion des plaintes, le travail de la CPVP présente des similitudes avec le travail du Médiateur. La loi du 8 décembre 1992 affirme en effet qu'une fois saisie d'une plainte recevable, la CPVP « accomplit toute mission de médiation qu'elle juge utile ». Elle tente de concilier les parties. En cas d'échec de la conciliation, elle émet un avis sur le caractère fondé de la plainte, qui peut être accompagné de recommandations. Par ailleurs, tout comme le Médiateur, la CPVP dispose du pouvoir de procéder à un examen sur place, d'exiger de se faire remettre tout document. Elle peut également dénoncer au procureur du Roi les infractions dont elle a connaissance[1393].

Néanmoins, quel critère permet au Médiateur de déterminer si la réclamation du citoyen concerne davantage la protection de ses données à caractère personnel – auquel cas elle doit être transmise à la CPVP – ou plutôt le fonctionnement général de l'administration – auquel cas elle est traitée par le Médiateur fédéral[1394] ?

[1388] *Ibid.,* art. 9.

[1389] D. RENDERS et T. BOMBOIS, « La médiation en droit public », *in La médiation. Voie d'avenir aux multiples facettes ou miroir aux alouettes ?* (dir. P.-P. RENSON), Louvain-la-Neuve, Anthemis, 2008, p. 156.

[1390] Sur cette institution et ses moyens d'action, voy. *infra,* Chapitre II.

[1391] Art. 31, §1er, de la loi du 8 décembre 1992.

[1392] Dans son rapport d'activité de 2008, le Médiateur indique avoir transmis 3 réclamations à la CPVP (voy. le rapport annuel de 2008, p. 22), et 2 en 2006 (voy. le rapport annuel de 2006, p. 33). Par contre, aucune réclamation n'a été transmise en 2010 ni en 2011.

[1393] Art. 32 de la loi du 8 décembre 1992.

[1394] Ou un autre médiateur si la question ne relève ni de la CPVP, ni du Médiateur fédéral.

> Par exemple, lorsqu'un contribuable se plaint du fait que le SPF Finances a versé de l'argent sur un mauvais numéro de compte, s'agit-il d'un problème de qualité des données à caractère personnel ou de fonctionnement du SPF Finances ? Les questions de ce type sont appelées à devenir de plus en plus nombreuses compte tenu de l'invasion de données à caractère personnel dans chaque administration, rendant délicate la frontière entre la compétence du Médiateur et de la CPVP. En effet, comme cela a déjà été dit, l'informatisation de l'administration se déployant, le régime de la protection des données à caractère personnel trouve de plus en plus à s'appliquer. Un nombre grandissant d'actes de l'administration implique donc l'application des règles de protection des données à caractère personnel. La délicate séparation entre la tâche du Médiateur et celle de la CPVP montre à nouveau combien il devient périlleux d'envisager la protection des données à caractère personnel comme un corps de règles distinct des droits constitutionnel et administratif traditionnels.

Il est difficile pour la médiateur d'apprécier sa compétence dans de tels cas. Cette difficulté est d'ailleurs grandissante au gré du développement de l'e-gouvernement[1395]. Pour l'heure, son appréciation est guidée par les deux critères traditionnellement utilisés pour toute réclamation.

Le premier critère est celui de savoir si l'administration visée est bien une *autorité administrative* fédérale, au sens de l'article 14 des lois coordonnées sur le Conseil d'État. C'est la raison pour laquelle le Médiateur fédéral n'est pas compétent pour connaître des réclamations introduites à l'encontre de la CPVP et des comités sectoriels instituées en son sein.

Le second critère est la *satisfaction du citoyen*. La formulation de la réclamation constitue à cet égard un bon indice.

Ainsi, si le citoyen se plaint du fait que sa vie privée a été violée par une administration, le Médiateur aura tendance à transmettre la plainte à la CPVP. On pense, par exemple, à un administré qui reprocherait à une administration de ne pas avoir fait droit à sa demande d'accéder à ses données à caractère personnel, en vertu de l'article 9 de la loi du 8 décembre 1992.

Si le citoyen se plaint du fait qu'il n'a pas reçu l'argent que lui doit le SPF Finances parce que le numéro de compte utilisé était erroné, le Médiateur traitera probablement le dossier, compte tenu du fait que la réclamation est motivée par la volonté du citoyen de récupérer son argent, et non une atteinte à sa vie privée. La plainte sera alors traitée au regard des règles générales du droit administratif, et non des règles de protection des données. Pourtant, ces dernières pourraient être appliquées vu que le numéro de compte est une donnée à caractère personnel. Elles offriraient

[1395] Entretien téléphonique avec un collaborateur du Médiateur fédéral, le 6 juillet 2012.

au Médiateur un certain nombre d'arguments d'autant plus convaincants qu'ils sont fondés sur des règles contraignantes[1396].

Néanmoins, ces deux critères n'empêchent pas que le Médiateur doive faire preuve d'une certaine subjectivité dans l'appréciation de sa compétence lorsqu'il est saisi de plaintes en lien avec l'e-gouvernement et doit donc juger si la plainte touche davantage au fonctionnement de l'administration, ou à la protection des données à caractère personnel.

415.- Le Médiateur, l'e-gouvernement et la recherche de solutions nouvelles. Le Médiateur a déjà rendu plusieurs recommandations en lien avec l'e-gouvernement, ayant jugé qu'elles ne devaient pas être transmises à la CPVP.

Dans ses recommandations, le Médiateur tente de trouver des solutions nouvelles, aptes à répondre aux problèmes générés par l'e-gouvernement. On constate que ces solutions s'inscrivent dans la lignée des règles prescrites par la protection des données à caractère personnel. Malheureusement, le Médiateur ne l'indique pas explicitement puisqu'il ne juge pas l'action administrative au regard de ce régime juridique.

> Par exemple, le Médiateur s'est prononcé sur l'*échange des données entre administrations*, à partir du cas d'un pensionné à qui l'administration reproche de ne pas l'avoir prévenue de son changement de statut. Le Médiateur constate que l'Administration des pensions peut accéder au Registre national ou au réseau de la Banque-Carrefour de la sécurité sociale pour savoir si le pensionné bénéficie d'une nouvelle pension supplémentaire. Dans sa recommandation 99/06, le Médiateur affirme que les principes de bonne administration, et plus particulièrement, « les principes de gestion contentieuse et du raisonnable », « requièrent [...] que les administrations concernées fassent usage des systèmes informatisés et automatisés existants ou en aménagent l'exploitation plutôt que de faire reposer sur le citoyen l'obligation parfois très lourde voire même impossible, de fournir lui-même un élément/une information/une preuve alors que l'administration dispose de moyens suffisants pour les obtenir par elle-même. Une mesure rappelant ce principe aux administrations s'avérerait salutaire ». En se penchant sur le régime juridique de la protection des données à caractère personnel, on constate que cette recommandation va dans le sens d'une véritable obligation légale existante, celle de la collecte unique des données, déjà ancrée jadis dans la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale.
>
> Nombre de cas soumis au Médiateur concernent aussi des *erreurs affectant les données* utilisées par l'administration, principalement le numéro de

[1396] Par exemple, un numéro de compte erroné viole l'article 4, 4°, de la loi du 8 décembre 1992, qui impose au responsable de traitement d'utiliser des données exactes et à jour.

compte bancaire repris sur l'avertissement-extrait de rôle[1397] ou l'adresse du contribuable[1398]. Le Médiateur invite alors l'administration à résorber ces erreurs administratives. Ce vœu du Médiateur correspond également à une obligation légale, celle d'utiliser des données à caractère personnel de qualité, comme le prescrit l'article 4, 4°, de loi du 8 décembre 1992 qui impose de ne traiter que les données exactes et à jour.

Dans le même sens, le Médiateur a souligné la difficulté de *trouver l'origine d'une erreur* affectant une information relative à un administré. « Trouver où et comment l'erreur a été commise revient presque à chercher une aiguille dans une botte de foin », notamment parce l'on est renvoyé d'une administration à l'autre[1399]. Il déplore qu'il n'y ait pas encore de solution pour rectifier les erreurs « immédiatement et [...] sans que cela ne présente d'inconvénient ou exige d'effort supplémentaire pour le contribuable »[1400] et invite l'administration à rectifier rapidement les erreurs. C'est pour cette raison notamment que nous avons insisté, dans le Titre 2 de la recherche, sur l'importance d'un cadastre d'interconnexions comme le prévoient déjà certaines législations sectorielles en matière de protection des données à caractère personnel[1401].

En d'autres termes, le Médiateur veille à ce que l'administration agisse conformément aux lois. Plus encore, il l'incite à perfectionner son action en respectant des principes de bonne administration et de bonne gouvernance, qui, même s'ils ne sont pas (ou pas encore) contraignants[1402], permettent d'améliorer la qualité du service public.

Reprenons un exemple précédent[1403]. Le Médiateur incite les administrations à mettre à jour les informations dont elles ont besoin grâce aux systèmes informatisés qui sont à leur disposition – tels qu'un accès à la Banque-Carrefour de la sécurité sociale. Il fonde sa recommandation, non sur une obligation légale, mais sur le principe de gestion contentieuse et le principe du raisonnable en vertu desquels on ne peut exiger des particuliers qu'ils fournissent eux-mêmes ces informations[1404]. Ces principes vont au-delà des obligations légales consacrées par le droit administratif.

1397 Voy. not. le rapport annuel 2008 pp. 34 et 35.

1398 *Ibid.*, p. 82.

1399 Voy. not. le rapport annuel de 2010, p. 90.

1400 *Idem.*

1401 Voy. *supra,* n°s 392.- et s.

1402 Comme nous l'avons souligné précédemment, certains principes de bonne administration et de bonne gouvernance peuvent acquérir une force contraignante une fois consacrés par le législateur (tel est le cas du principe de motivation des actes administratifs) ou reconnus comme des principes généraux du droit par la jurisprudence, et assortis d'une sanction. Sur ce phénomène, voy. P.-Y. Monette, *op. cit,* pp. 18 à 21.

1403 Voy. *supra,* n° 415.-

1404 RG 99/06.

Deux suggestions s'imposent aux termes de ces développements.

La première suggestion s'adresse au Médiateur. Les recommandations qui, pour l'heure, sont justifiées par des principes de bonne administration, de bonne gouvernance ou d'équité gagneraient à être nourries par une référence explicite au régime de la protection des données à caractère personnel. Elles seraient alors fondées sur des obligations légales contraignantes et n'en seraient que plus convaincantes.

La deuxième suggestion concerne les administrations. Tant les recommandations fondées sur le respect des règles contraignantes du droit administratif que celles fondées sur les principes de bonne administration, de bonne gouvernance et d'équité, vont dans le sens du régime de la protection des données à caractère personnel. Cela signifie que les administrations doivent sans crainte se conformer pleinement au régime de la protection des données à caractère personnel. Non seulement, ces obligations ne sont pas contraires au droit administratif et auxdits principes, mais plus encore, elles s'inscrivent dans le même souci d'assurer une relation équilibrée entre les particuliers et l'administration[1405].

B. Les autorités consultatives

416.- Considérations générales. La section de législation du Conseil d'État et la Commission d'accès aux documents administratifs[1406] sont amenées à rendre des avis à propos de l'e-gouvernement. Leurs enseignements apportent un éclairage utile pour interpréter le droit administratif au regard des questions nouvelles engendrées par l'informatisation de l'administration.

§1. La section de législation du Conseil d'État

417.- La présentation de la section de législation du Conseil d'État. La section de législation du Conseil d'État est un organe consultatif composé de douze membres du Conseil d'État et de dix assesseurs au maximum[1407]. Elle exerce une compétence d'avis sur les normes en

[1405] À cet égard, par exemple, on a souligné précédemment la convergence entre la transparence administrative et la transparence des traitements de données à caractère personnel. Voy. *supra*, n° 378.-

[1406] Ci-après, « CADA ».

[1407] Sur la composition de la section de législation du Conseil d'État, voy. les articles 79 à 83 des lois du 12 janvier 1973 coordonnées sur le Conseil d'État (*M.B.,* 21 mars 1973), ci-après « Lois coordonnées sur le Conseil d'État ». Signalons que les règles de procédure à suivre pour demander l'avis de la section de législation du Conseil d'État sont ancrées

projet. Grâce à ce mécanisme, les normes organisant des traitements de données à caractère personnel au sein du secteur public sont confrontées notamment aux exigences du droit administratif. Ce contrôle est utile, mais parcellaire.

1. Un contrôle utile

418.- Des avis éclairants. Les avis de la section de législation du Conseil d'État constituent une précieuse source d'informations pour la compréhension du régime juridique applicable à l'e-gouvernement[1408]. Il en va d'autant plus ainsi que la jurisprudence de la Cour constitutionnelle, celle du Conseil d'État, ainsi que les décisions des cours et tribunaux, sont encore rares en cette matière, tout comme la doctrine publiciste commentant ces évolutions récentes.

419.- L'article 22 de la Constitution et la compétence de l'auteur de la réglementation. En matière d'e-gouvernement, on constate que la section de législation du Conseil d'État se concentre principalement sur les questions liées à la compétence de l'auteur de la réglementation et ce, à la lumière de l'article 22 de la Constitution et des normes supranationales applicables à la protection des données à caractère personnel.

Ainsi, la section de législation confronte l'article 22 de la Constitution au principe de la *séparation des pouvoirs*. À cette occasion, elle opère notamment une distinction utile entre les aspects de l'e-gouvernement qui doivent être réglés par le législateur, en vertu de l'exigence de légalité, de celles qui peuvent être organisées par le Roi, en vertu de son pouvoir d'exécution des lois[1409].

---

dans une circulaire de la Chancellerie du Premier Ministre datée du 10 septembre 2004. Elle est disponible sur le site du Conseil d'État, à l'adresse http://www.raadvst-consetat.be/?page=procedure&lang=fr

[1408] En ce sens, d'aucuns affirment que l'argumentation fouillée des avis de la section de législation du Conseil d'État s'explique par le fait que ces avis sont purement consultatifs et ne doivent pas être obligatoirement suivis. Cette autorité doit donc « convaincre pour être suivie. Elle est contrainte d'argumenter davantage » [P. VANDERNACHT et X. DELGRANGE, « Ebauche d'une comparaison des contrôles préventif de la section de législation du Conseil d'État et curatif de la Cour d'arbitrage », *in Le Conseil d'État de Belgique. Cinquante ans après sa création (1946-1996)* (dir. B. BLERO), Bruxelles, Bruylant, 1999, p. 141].

[1409] *Cf. supra*, n° 86.- Voy., not., SLCE, avis du 27 avril 1989 relatif à un projet de loi instituant une Banque-Carrefour de la sécurité sociale, *Doc. Parl.,* Ch. Repr., sess. 1988-1989, n° 899/1, p. 101 ; SLCE, avis n° 33.285/1 du 2 mai 2002 relatif à un avant-projet de loi portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce et création des guichets d'entreprise, *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50-2058/001, p. 103 ; SLCE, avis n° 41.662/1/2/3/4 des 14, 16 et 17 novembre

La section de législation accorde également une attention particulière au lien entre l'article 22 de la Constitution et le principe de la *répartition des compétences* entre la collectivité fédérale et les collectivités fédérées.

Nombre d'avis sont ainsi consacrés à la question de savoir si les décrets et les ordonnances portant sur la protection des données à caractère personnel sont soumis au respect de la loi du 8 décembre 1992[1410]. En outre, la section de législation du Conseil d'État ne manque pas de rappeler régulièrement l'intérêt de recourir aux accords de coopération au moment d'organiser l'e-gouvernement puisque cette matière implique une grande collaboration entre les institutions qui s'échangent des données à caractère personnel, qu'elles soient fédérales, communautaires ou régionales. En effet, l'administration fédérale et les administrations des entités fédérées doivent pouvoir s'échanger les données enregistrées dans les sources authentiques qu'elles détiennent, comme l'a montré le premier titre de la recherche. Or, le législateur fédéral excèderait ses compétences s'il venait à imposer des obligations à des institutions qui ne relèvent pas de l'autorité fédérale[1411].

Par ailleurs, la section de législation du Conseil d'État se prononce également sur le *type d'instrument législatif utilisé*. Elle décourage ainsi le recours à la loi-programme pour modifier des règles essentielles de l'e-gouvernement, telles que celles contenues dans la loi du 8 décembre 1992 ou la loi du 8 août 1983 relative au Registre national[1412].

2006 relatif à un avant-projet de loi-programme, *Doc. Parl.,* Ch. Repr., sess. 2006-2007, n° 2773/002, p. 425 ; SLCE, avis n° 44.192/1 du 1er avril 2008 *over een voorontwerp van decreet betreffende het elektronische bestuurlijke gegevensverkeer, Doc.,* Parl. Fl., sess. 2007-2008, n° 1712/1, p. 130 ; SLCE, avis du 27 mars 1996 sur un projet de loi organique des services de renseignements et de sécurité, *Doc. Parl.,* Sénat, sess. 1995-1996, n° 638/1, pp. 29 à 34 ; SLCE, avis n° 37.765/1/2/3/4 sur un avant-projet de « loi-programme », *Doc. Parl.,* Ch. Repr., sess. 2004-2005, n° 51-1437/002, p. 634 ; SLCE, avis n° 47.162/4 du 2 décembre 2009, *Doc. Parl.,* Ch. Repr., sess. 2009-2010, n° 52-2493/001, p. 43 ; SLCE, avis du 14 septembre 2000 sur un avant-projet de loi relative à la Centrale des Crédits aux Particuliers, *Doc. Parl.,* Ch. Repr., sess. 2000-2001, n° 50-1123/001, pp. 33 et 34.

Voy. not. SLCE, avis n° 33.962/2, *op. cit.,* p. 15 ; SLCE, avis n° 37.288/3 des 6, 12 et 15 juillet 2004 *over een voorontwerp van decreet betreffende het gezondheidsinformatiesysteem, Doc.,* Parl. fl., sess. 2005-2006, n° 531/1, p. 163 ; SLCE, avis n° 42.034/2, *op. cit.,* pp. 6 et 7.

[1410] À ce sujet, voy. *supra,* nos 80.- et s.

[1411] Voy. not. SLCE, avis n° 33.962/2, *op. cit.,* p. 15 ; SLCE, avis n° 37.288/3 des 6, 12 et 15 juillet 2004 *over een voorontwerp van decreet betreffende het gezondheidsinformatiesysteem, Doc.,* Parl. fl., sess. 2005-2006, n° 531/1, p. 163 ; SLCE, avis n° 42.034/2, *op. cit.,* pp. 6 et 7.

[1412] SLCE, avis des 10, 11, 12 et 13 octobre 2004 sur un avant-projet de loi portant des dispositions sociales et diverses, *Doc. Parl.,* Sénat, sess. 1994-1995, n° 1218/1, p. 255 ; SLCE, avis n° 37.765/1/2/3/4, *op. cit.,* p. 633.

> La section de législation du Conseil d'État rappelle que « la nécessité éventuelle [...] d'adopter rapidement des dispositions dans des matières qui touchent directement aux libertés des personnes ne peut, en principe, être admise pour justifier le recours au procédé des lois-programmes en ce domaine »[1413].

420.- La défense du rôle de la CPVP. Comme il en sera fait état dans la section suivante, les normes organisant des traitements de données peuvent être soumises à l'avis de la CPVP, en sus de l'examen mené par la section de législation du Conseil d'État. Néanmoins, la consultation de la CPVP n'est donc pas une formalité obligatoire.

Pour autant, la section de législation du Conseil d'État ne manque pas de souligner régulièrement l'importance des avis de la CPVP et l'utile complémentarité qu'ils présentent par rapport à son propre travail. Ainsi, bien que la consultation de la CPVP ne soit pas obligatoire, elle est vivement encouragée.

> Selon les termes de la section de législation du Conseil d'État, la consultation de la CPVP est « un gage de bonne procédure législative »[1414], qui est « vivement souhaitable [...] du point de vue d'une bonne administration »[1415]. En outre, la section de législation suggère de joindre au texte en projet « lors de son dépôt au Parlement, les avis de la CPVP utiles à la bonne compréhension des dispositions en projet »[1416], de manière à « clarifier la portée [du texte]

[1413] SLCE, avis des 10, 11, 12 et 13 octobre 2004 sur un avant-projet de loi portant des dispositions sociales et diverses, *Doc. Parl.,* Sénat, sess. 1994-1995, n° 1218/1, p. 255.

[1414] SLCE, avis n° 39.813/3 du 14 février 2006 cité par CPVP, avis n° 25/2006 du 12 juillet 2006 relatif à un projet de modification du point 15° de l'art. 4, B, de l'annexe V de l'arrêté du Gouvernement flamand du 18 décembre 1998 portant agrément et subventionnement des associations et des structures d'aide sociale dans le cadre des soins à domicile, p. 3, n° 11.

[1415] SLCE, avis des 7 et 8 décembre 1995 relatif à un avant-projet de loi sociale, *Doc. Parl.,* Sénat, sess. 1995-1996, n° 352/1, p. 131. Voy. dans le même sens, SLCE, avis n° 34.270/1 du 23 janvier 2003, cité par CPVP, avis n° 15/2006 du 14 juin 2006 relatif au projet d'arrêté royal réglant la collaboration à l'association chargée de l'enregistrement du kilométrage des véhicules, p. 2, n° 4 ; SLCE, avis n° 39.340/2 du 14 décembre 2005, relatif à une proposition de loi réglant l'installation et l'utilisation de caméras de surveillance et de sécurité dans les lieux ouverts, *Doc. Parl.,* Ch. Repr., sess. 2005-2006, n° 51-2038/002, p. 12 ; SLCE, avis n° 42.014/4 du 15 janvier 2007, cité par CPVP, avis n° 09/2007 du 21 mars 2007 quant au projet d'arrêté royal relatif au permis de conduire, à l'aptitude professionnelle et à la formation continue des conducteurs de véhicules des catégories C, C+E, D, D+E et des sous-catégories C1, C1+E, D1, D1+E, p. 2, n° 2.

[1416] SLCE, avis n° 33.962/2 des 18 et 19 novembre 2002 relatif à l'avant-projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50-2226/003, p. 3.

et identifier les principes juridiques auxquels il doit satisfaire, sans avoir à consulter le site électronique de la Commission de la vie privée »[1417].

2. Un contrôle parcellaire

421.- Consultation facultative et avis non contraignant. La section de législation du Conseil d'État ne se prononce pas sur l'ensemble de la réglementation de l'e-gouvernement.

D'une part, la consultation de la section de législation n'est pas toujours obligatoire. Elle peut également être assortie d'un délai qui contraint l'autorité consultative à limiter l'étendue de son examen.

D'autre part, les avis de la section de législation du Conseil d'État ne sont pas contraignants. L'auteur du texte en projet est libre de les suivre, ou pas, sans qu'il doive justifier son choix.

422.- La saisine obligatoire ou facultative de la section de législation du Conseil d'État. L'obligation de consulter cette autorité ne vise que certains textes en projet. D'autre part, même lorsque la section de législation du Conseil d'État est consultée, son travail peut être affecté par l'invocation de délais parfois très courts qui imposent de réduire le champ de l'analyse menée.

a) La limitation de l'obligation de consulter la section de législation du Conseil d'État. L'article 2 des Lois coordonnées sur le Conseil d'État prévoit que seuls les avant-projets de loi, de décret et d'ordonnance, ainsi que les projets de normes de valeur réglementaire, doivent être soumis à l'avis de la section de législation du Conseil d'État, sans condition[1418].

Les propositions de loi, de décret et d'ordonnance, ainsi que les amendements à des projets ou des propositions, ne sont soumis à la consultation obligatoire de l'organe d'avis que si un tiers au moins des membres de l'assemblée législative concernée en fait la demande. Les propositions de loi et d'ordonnance, ainsi que les amendements à des projets ou des propositions doivent également être soumis à la section de législation du Conseil d'État si la majorité d'un groupe linguistique en fait la demande.

[1417] SLCE, avis n° 37.943/2 du 11 janvier 2005 relatif à un avant-projet de loi instituant le système d'information Phénix, *Doc. Parl.,* Ch. Repr., sess. 2004-2005, n° 51-1645/001, p. 40.

[1418] Il est fait exception à ce principe pour les projets relatifs aux budgets, comptes, emprunts, opérations domaniales et contingent de l'armée ou lorsque l'urgence motivée est invoquée.

Par ailleurs, un avis doit être sollicité pour les projets et propositions de loi, ainsi que « les amendements, adoptés lors d'une premier vote, à des projets ou propositions de loi », lorsque la demande de consultation est fondée sur l'article 16 de la loi du 6 avril 1995 organisant la commission parlementaire de concertation prévue à l'article 82 de la Constitution.

Compte tenu des hypothèses limitées dans lesquelles la consultation est obligatoire, certaines normes régissant des aspects substantiels de l'e-gouvernement n'ont pas bénéficié de l'analyse juridique du Conseil d'État.

> Par exemple, une loi du 26 février 2003[1419] a apporté des modifications importantes à l'organisation de la protection des données dans l'administration. Elle n'a pas été soumise à la section de législation du Conseil d'État, ayant été introduite par une proposition de loi. Pourtant, cette loi modifie notamment le statut de la CPVP et en faire un organe collatéral de la Chambre des représentant. Plus encore, elle crée des comités sectoriels, qui sont des organes de contrôle institués au sein de la CPVP, ayant un pouvoir de décision semblable à celui d'une autorité administrative[1420]. Ces modifications génèrent aujourd'hui d'âpres difficultés, comme le montre la section qui suit. Ces difficultés auraient peut-être pu être évitées grâce à une analyse juridique pertinente de la section de législation du Conseil d'État.

b) La saisine assortie de délais. La section de législation du Conseil d'État est parfois contrainte de limiter l'objet de son analyse, lorsque l'avis doit être rendu dans un délai de 5 jours ou de 30 jours.

En effet, en vertu de l'article 84, §1er, 1°, des Lois coordonnées sur le Conseil d'État, l'autorité qui saisit la section de législation du Conseil d'État peut réclamer la communication de l'avis dans un *délai de 30 jours*. Dans ce cas, l'organe consultatif « peut se borner à l'examen de la compétence de l'auteur de l'acte, du fondement juridique ainsi que de l'accomplissement des formalités prescrites », comme le lui autorise l'article 84, §3, desdites Lois coordonnées.

L'avis peut également être réclamé dans un *délai de 5 jours*, en cas d'urgence motivée dans la demande d'avis et ce, en vertu de l'article 84, §1er, alinéa 1er, 2°, des Lois coordonnées. Dans cette hypothèse, l'examen de la section de législation est nécessairement limité aux aspects précités, énoncés à l'article 84, §3.

[1419] Loi du 26 février 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP.

[1420] Voy. *infra*, nos 534.- et s.

Malheureusement, nombre de demandes relatives à des normes organisant l'e-gouvernement réclament que l'avis soit rendu dans un de ces délais, si bien que des pans de la matière ne reçoivent pas l'appréciation juridique de la section de législation du Conseil d'État.

> En guise d'illustration, sur 16 avis rendus par la section de législation à propos de normes régissant des aspects importants de l'e-gouvernement[1421], 12 d'entre eux ont été rendus dans un délai particulier. Le délai de 30 jours était réclamé pour 6 avis. Le délai de 5 jours concernait 3 avis tandis que 3 avis ont été rendus dans un délai de 3 jours[1422].

Ces avis renferment nécessairement des silences, liés au peu de temps dont disposait la section de législation pour se prononcer. Comme l'affirme

---

[1421] Il s'agit des avis suivants : SLCE, avis n° 33.962/2 des 18 et 19 novembre 2002 relatif à l'avant-projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques précité ; SLCE, avis du 27 avril 1989 relatif à un projet de loi instituant une Banque-Carrefour de la sécurité sociale, précité ; SLCE, avis n° 33.285/1 du 2 mai 2002 relatif à un avant-projet de loi portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce et création des guichets d'entreprise, précité ; SLCE, avis n° 41.662/1/2/3/4 des 14, 16 et 17 novembre 2006 relatif à un avant-projet de loi-programme, précité ; SLCE, avis du 28 novembre 1990 concernant le projet de loi « relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. Parl.,* Ch. Repr., sess. 1990-1991, n° 1610/1, pp. 50-68 ; SLCE, avis des 31 mai 1996 et 4 juin 1996 sur un avant-projet de loi « portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions », *Doc. Parl.,* Ch. Repr., sess. 1995-1996, n° 607/1, pp. 54-80 ; SLCE, avis n° 44.192/1 du 1er avril 2008 over een voorontwerp van decreet betreffende het elektronische bestuurlijke gegevensverkeer, précité ; SLCE, avis n° 37.288/3 des 6, 12 et 15 juillet 2004 over een voorontwerp van decreet betreffende het gezondheidsinformatiesysteem, précité ; SLCE, avis n° 37.765/1/2/3/4 sur un avant-projet de « loi-programme », précité ; SLCE, avis n° 37.766/1/2 du 4 novembre 2004 sur un avant-projet de lio « portant des dispositions diverses », *Doc. Parl.,* Ch. Repr., sess. 2004-2005, n° 51-1437/002, pp. 642652 ; SLCE, avis du 12 janvier 1995 relatif à une proposition de loi « réglant la libre collecte d'informations », *Doc. Parl.,* Sénat, sess. 1994-1995, n° 1635/2, pp. 1-18 ; SLCE, avis n° 37.943/2 du 11 janvier 2005 relatif à un avant-projet de loi instituant le système d'information Phénix, précité ; SLCE, avis n° 42.034/2 du 24 janvier 2007, portant sur un avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service Public Fédéral Finances, précité ; SLCE, avis n° 47.162/4 du 2 décembre 2009 relatif à l'avant-projet de loi portant création de la Banque-Carrefour des véhicules, précité ; SLCE, avis des 10, 11, 12 et 13 octobre 2004 sur un avant-projet de loi portant des dispositions sociales et diverses, précité ; SLCE, avis des 7 et 8 décembre 1995 relatif à un « avant-projet de loi sociale », précité.

[1422] Signalons que le délai de 3 jours était prévu par les Lois coordonnées avant leur modification par la loi du 2 avril 2003. Il a été remplacé le délai de 5 jours (voy. la Loi du 2 avril 2003 modifiant certains aspects de la législation relative à l'organisation et au fonctionnement de la section de législation du Conseil d'État, *M.B.,* 14 mai 2003).

elle-même l'autorité consultative dans son avis relatif à un avant-projet de loi portant création de la Banque-Carrefour des entreprises, « l'absence d'observation concernant l'une ou l'autre disposition du projet ne signifie pas que le texte du projet ne soit ni critiquable, ni perfectible. Il va de soi que le silence gardé par la section de législation sur ces dispositions ne pourrait servir d'élément d'interprétation du projet de loi »[1423].

Un tel constat laisse perplexe, d'aucuns affirmant que « l'on ne peut écarter l'hypothèse que, lorsque les auteurs de projets ou de propositions ont conscience de prendre quelque liberté avec la Constitution, ils préfèrent ne pas laisser à la section de législation le temps d'examiner leur texte dans le détail »[1424]. S'agissant des normes régissant l'e-gouvernement, cette interrogation ne manque pas d'interpeller, au vu des critiques de constitutionnalité adressées à certaines lois régissant actuellement l'e-gouvernement[1425].

423.- Des avis non contraignants. Le législateur et le Gouvernement ne sont pas juridiquement contraints de suivre l'avis de la section de législation du Conseil d'État ni même de faire figurer dans les travaux préparatoires de la norme en projet, une justification du refus éventuel de suivre ces recommandations.

On constate ainsi que nombre d'avis rendus en matière d'e-gouvernement ne sont pas suivis par l'auteur de la norme en projet. De plus, l'exposé des motifs de ces normes contient rarement une réelle justification d'une telle attitude[1426].

> Entre autres exemples, le précédent titre de la recherche relatif à la transparence de l'e-gouvernement[1427], a fait état de l'ancien article 20, §1, 1°, de la loi sur la Banque-Carrefour de la sécurité sociale, qui prévoyait l'obligation, pour les institutions de sécurité sociale, de communiquer « aux bénéficiaires de la sécurité sociale [...] les données sociales à caractère personnel sur lesquelles elles se sont basées pour la détermination ou l'appréciation de leurs droits ». À cette occasion, nous avons démontré l'intérêt d'une telle disposition pour la transparence des échanges de données entre institutions publiques qui fondent des décisions administratives. Comme on l'a dit éga-

[1423] SLCE, avis n° 33.285 précité, p. 101.

[1424] P. VANDERNACHT et X. DELGRANGE, *op. cit.,* p. 123.

[1425] Voy. *supra,* Titre I.

[1426] Ce constat s'étend aux avis de la section de législation en général, quelle que soit la matière concernée (voy. à ce sujet, B. JADOT et J. VAN NIEUWENHOVE, « De afdeling wetgeving van de Raad van State gezien van binnenuit – La section de législation du Conseil d'État, vue de l'intérieur », *in De adviesbevoegdheid van de Raad van State – La compétence d'avis du Conseil d'État* (dir. L. WINTGENS), Brugge, die Keure, 2003, pp. 65-66).

[1427] Voy. *supra,* n° 318.-

lement, cette disposition a été remplacée par un renvoi à la loi du 29 juillet 1991 relative à la motivation formelle des actes administratif.

La section de législation du Conseil d'État s'était opposée à une telle modification, jugeant notamment qu'il s'agissait d'un recul dans la transparence des traitements de données à caractère personnel puisque ni ladite loi du 29 juillet 1991 ni la loi du 8 décembre 1992 ne prévoyaient une obligation de communiquer les données utilisées lors de l'adoption d'une décision administrative[1428].

Cette modification a pourtant été adoptée. L'exposé des motifs ne contient aucune réponse à l'avis de la section de législation sur ce point, et n'évoque même pas l'existence de critiques de la part de l'organe consultatif[1429].

Par ailleurs, les justifications que contient ce même exposé des motifs à propos d'autres dispositions prévues en matière de sécurité sociale s'avèrent bien sommaires eu égard à l'importance de certaines critiques émises par la section de législation du Conseil d'État. Ainsi, en réponse au Conseil d'État qui suggérait d'habiliter le Roi à déterminer le contenu de la nouvelle banque de données pensions organisée par la réglementation examinée, il a été soutenu qu'une telle suggestion « n'a pas été retenue car un tel formalisme est contraire à la souplesse nécessaire à une gestion efficiente des données de sécurité sociale ». Force est de constater qu'il s'agit là d'un raisonnement rapide, fondé exclusivement sur l'impératif d'efficacité administrative, au mépris de la protection de la vie privée des citoyens.

Dans le même sens, constatant que ce texte prévoyait des règles en matière de traitements de données, distinctes de celles prévues par la loi du 8 décembre 1992, la section de législation avait recommandé de consulter la CPVP. L'auteur du projet de loi a soutenu, sans nuance, que ces dispositions, instituant notamment une base de données nouvelle, « ne portent pas atteinte aux principes fondamentaux de la protection de la vie privée »[1430].

424.- Des solutions envisageables. On peut raisonnablement penser que le manque de prise en compte des avis de la section de législation du Conseil d'État est lié au fait que ceux-ci interviennent tardivement dans le processus d'élaboration des normes législatives ou réglementaires. Le manque de temps et de volonté pour modifier les normes dont la rédaction est déjà très avancée pourrait expliquer aussi le peu d'attention et de soin accordé aux réponses données à ces avis dans l'exposé des motifs.

[1428] SLCE, avis des 7 et 8 décembre 1995 relatif à un « avant-projet de loi sociale », *op. cit.,* p. 132. Voy. *supra,* n° 420.-

[1429] Voy. Projet de loi portant des dispositions diverses, Exposé des motifs, *Doc. Parl.,* Ch. Repr., sess. 1995-1996, n° 352/1, pp. 43-44.

[1430] *Ibid.,* p. 18.

Des solutions sont envisageables, qui portent sur le moment de la consultation de la section de législation du Conseil d'État et sur les justifications à apporter lorsque ses avis ne sont pas suivis.

a) Le moment de la consultation. On pourrait imposer la consultation de la section de législation du Conseil d'État dès le début du processus législatif[1431]. D'une part, cette obligation empêcherait la saisine assortie de délais qui réduit bien souvent la portée des avis. D'autre part, des questions ciblées de droit administratif pourraient ainsi être soumises au Conseil d'État. Les réponses de ce dernier constitueraient alors des balises juridiques au sein desquelles pourrait utilement œuvrer l'auteur de la norme.

b) Les justifications suite à la consultation. Lorsque l'auteur d'une norme décide de ne pas suivre l'avis de la section de législation du Conseil d'État, les justifications de ce choix sont intéressantes à deux égards au moins. D'une part, ces explications enrichissent les travaux préparatoires de la norme adoptée, et permettent à tout un chacun de comprendre pourquoi des remarques du Conseil d'État, *a priori* pertinentes, n'ont pas été suivies concrètement. D'autre part, la formulation de justifications incite l'auteur de la norme à réfléchir au bien fondé de son choix et à la qualité juridique des règles qu'il adopte. Dès lors, il pourrait être envisagé d'imposer à l'auteur d'une norme examinée par la section de législation du Conseil d'État de répondre à chacune des remarques formulées par cette autorité. Ces justifications figureraient dans l'exposé des motifs d'une norme législative en projet, ou dans le préambule d'une norme réglementaire[1432].

§2. La Commission d'accès aux documents administratifs

425.- Une section de la Commission d'accès aux et de réutilisation des documents administratifs. La Commission d'accès aux documents

[1431] En ce sens, B. Jadot et J. Van Nieuwenhove, *op. cit.*, p. 71 ; J. Velaers, « Het preventieve grondwettigheidstoezicht van de Raad van State in het raam van de kwaliteitszorg voor wetgeving », *in Wie maakt over de kwaliteit van de wet ? Het wetgevingsbeleid in België* (dir. M. Adams en G. Popelier), Anvers, Intersentia Rechtswetenschappen, 2000, pp. 227 et s. ; B. Jadot, « La section de législation du Conseil d'État et l'élaboration de la règle de droit », *in Elaborer la loi aujourd'hui, mission impossible ?* (dir. B. Jadot et F. Ost), Bruxelles, Facultés universitaires Saint-Louis, 1999, pp. 165 et s. ; X. Delgrange, L. Detroux et H. Dumont, « La régulation en droit public », *op. cit.*, p. 49.

[1432] En ce sens, B. Jadot et J. Van Nieuwenhove, *op. cit.*, p. 66, qui mentionnent, en note 3, qu'une telle obligation existe aux Pays-Bas. Le gouvernement hollandais rédige un rapport dans lequel il répond à la section de législation. Ce rapport est publié dans un document parlementaire, en annexe de l'avis de la section de législation.

administratifs[1433] est une des deux sections qui composent la Commission d'accès aux et de réutilisation des documents administratifs, la deuxième section étant la Commission de réutilisation des documents administratifs[1434].

Ces deux sections sont néanmoins instituées par deux lois distinctes. La *CADA* est instituée par la loi du 11 avril 1994 sur la publicité de l'administration tandis que la *Commission de réutilisation des documents administratifs* trouve son fondement dans la loi du 7 mars 2007 sur la réutilisation des documents administratifs[1435]. Ces deux sections sont organisées par le même arrêté royal pour assurer une meilleure cohérence entre elles, comme l'avait suggéré la section de législation du Conseil d'État[1436]. Seule la CADA retiendra notre attention dans les développements qui suivent[1437].

La Commission d'accès aux et de réutilisation des documents administratifs est un organe du pouvoir exécutif établi auprès du SPF Intérieur. Elle est composée pour moitié de fonctionnaires et pour l'autre moitié de personnes n'ayant pas cette qualité. Tous sont nommés par le Roi qui peut mettre fin à leur mandat dans certaines hypothèses[1438].

Cette institution exerce sa mission de manière indépendante, ce qui explique que les membres de cette commission ne peuvent recevoir d'instruction de personne[1439] ni se prononcer sur les dossiers à l'égard desquels ils ne seraient pas impartiaux[1440].

1433 Ci-après, « CADA ».

1434 Voy. l'arrêté royal du 29 avril 2008 relatif à la composition et au fonctionnement de la Commission d'accès aux et de réutilisation des documents administratifs, *M.B.,* 8 mai 2008.

1435 Loi du 7 mars 2007 transposant la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public.

1436 Rapport au Roi précédent l'arrêté royal du 29 avril 2008 précité.

1437 Deux raisons expliquent que la Commission de réutilisation des documents administratifs n'est pas étudiée dans le cadre de cette recherche. D'une part, elle est se prononce sur « l'utilisation de documents administratifs dont les autorités publiques disposent, à des fins commerciales ou non commerciales, autres que l'objectif initial de la mission de service public pour lequel les documents administratifs ont été produits » (art. 2, 4°, de la loi du 7 mars 2007). Or, notre recherche se concentre sur l'exécution des missions de service public. C'est pourquoi, on n'étudie pas la réutilisation de données personnelles pour satisfaire à une finalité commerciale, notamment. D'autre part, ladite loi du 7 mars 2007 dispose que, lorsque ces documents contiennent des données à caractère personnel, ils doivent être anonymisés. Or, notre recherche porte principalement sur la protection des données à caractère personnel non anonymisées.

1438 Voy. les art. 4 à 7 de l'arrêté royal du 29 avril 2008 précité.

1439 *Ibid.,* art. 8.

1440 *Ibid.,* art. 16.

426.- Une compétence d'avis. La CADA exerce une compétence d'avis concernant l'application de la loi du 11 avril 1994 qui, rappelons-le, organise l'accès aux documents administratifs[1441].

Tout comme le contrôle exercé par la section de législation du Conseil d'État, le contrôle qu'effectue la CADA est utile mais parcellaire.

1. Un contrôle utile

427.- Transparence administrative et transparence des traitements de données à caractère personnel. En veillant au respect de la loi du 11 avril 1994 qui organise l'accès aux documents administratifs, la CADA œuvre à la transparence administrative en général. Elle n'est pas compétente pour contrôler le respect, par l'administration, des règles de transparence organisées par le régime juridique de la protection des données. Cette mission est dévolue à la CPVP[1442].

Néanmoins, l'action de la CADA intéresse directement la transparence des traitements de données. En effet, nombre de documents administratifs contiennent des informations très pertinentes pour comprendre, *in abstracto,* les traitements de données à caractère personnel effectués dans l'administration. À cet égard, le document que constitue la « table des données disponibles » et qui est détenu par la Banque-Carrefour de la sécurité sociale est un exemple parlant. L'accès offert par la loi du 11 avril 1994 et contrôlé par la CADA est la seule voie existant actuellement pour prendre connaissance de ce type de document[1443].

Malheureusement, jusqu'à présent, la CADA a été peu sollicitée au sujet de la transparence de l'e-gouvernement. Néanmoins, dans le cadre de cette recherche, nous avons sollicité la CADA à deux reprises au sujet de problématiques liées à l'e-gouvernement. La première demande d'avis que nous avons introduite à la CADA concerne le refus de la Banque-Carrefour de la sécurité sociale de nous donner accès à la table des données disponibles au sein du réseau de la sécurité sociale[1444], outil cardinal de l'e-gouvernement que nous venons d'évoquer. Elle a donné lieu à l'avis

[1441] Cette loi a fait l'objet de longs développements dans la Titre II de la présente recherche.

[1442] Voy. *infra,* n°s 487.- et s.

[1443] Rappelons, en effet, qu'en exerçant le droit d'accès organisé par la loi du 8 décembre 1992, la personne concernée ne peut prendre connaissance que de la localisation de ses propres données au sein du réseau sectoriel de la sécurité sociale, mais ne peut pas prétendre à l'obtention de la table de localisation des données. Voy. *supra,* n°s 324.- et s.

[1444] Voy. *supra,* n° 299.-

n° 2010-41[1445]. La deuxième demande d'avis soumise à la CADA concerne l'application du régime de la transparence administrative à la CPVP. Elle a donné lieu à l'avis n° 2011-309[1446]. Il en sera question plus loin[1447].

428.- Demande de reconsidération et recours au Conseil d'État. La procédure prévue pour obtenir l'avis de la CADA est intéressante[1448]. En effet, un citoyen ne peut demander l'avis de la CADA qu'à la condition d'introduire, dans le même temps, une demande de reconsidération auprès de l'administration qui a refusé l'accès au document administratif recherché. De cette manière, l'administration est incitée à revoir sa décision, sans que le citoyen puisse être considéré comme un « harceleur » puisque telle est la procédure légale.

En outre, une fois émis l'avis de la CADA, cette dernière le communique à l'administration concernée qui est ainsi mise au courant de la légalité ou de l'illégalité de son attitude, le cas échéant. En cas d'illégalité, si elle refuse à nouveau l'accès demandé, un recours au Conseil d'État peut être introduit contre ce deuxième refus. L'avis de la CADA, joint au dossier, est susceptible d'éclairer utilement les conseillers.

2. Un contrôle parcellaire

429.- Deux causes. La CADA ne peut effectuer qu'un contrôle parcellaire de l'e-gouvernement. Cela tient aux limites imposées par la loi du 11 avril 1994 et à la faiblesse de ses moyens d'action.

430.- Les limites de la loi du 11 avril 1994. Le contrôle de la CADA est parcellaire, principalement à cause des limites qu'impose la loi du 11 avril 1994 à la transparence de l'administration, comme il en a été question dans le Titre II de cette recherche. On pense particulièrement au fait que seules les autorités administratives au sens de l'article 14 des lois coordonnées sur le Conseil d'État sont soumises à ce régime, ainsi qu'aux nombreuses exceptions dont cette loi assortit le principe de transparence[1449].

[1445] CADA, avis n° 2010-41 du 12 juillet 2010, sur le refus de donner accès à la table des données disponibles au sein du réseau sectoriel de la sécurité sociale, disponible sur le site www.documentsadministratifs.be

[1446] CADA, avis n° 2011-309 du 10 octobre 2011 sur le refus de donner accès à des documents qui ont été utilisés par le Comité sectoriel de la sécurité sociale et des la santé pour prendre une décision, disponible sur le site www.documentsadministratifs.be

[1447] Voy. *infra*, n°s 522.- et 580.-

[1448] Art. 8 de la loi du 11 avril 1994 précitée.

[1449] Voy. *supra*, n°s 263.- et s.

431.- De faibles moyens d'action. La CADA n'a pas de pouvoir de décision, ni de sanction, ce qu'elle déplore d'ailleurs.

Ainsi, bien que la CADA ait rendu un avis favorable à notre demande d'accès à la table des données disponibles, la Banque-Carrefour de la sécurité sociale n'a pas voulu nous en donner copie, prétextant soudainement, en réponse à notre demande de reconsidération, qu'elle ne disposait pas de cette table, ce qu'elle n'avait pourtant pas mentionné dans sa première réponse à notre demande d'accès[1450].

Face à pareille attitude, la CADA est dépourvue de moyens. Elle peut, certes, « consulter sur place toutes les informations utiles ou se les faire communiquer par l'autorité administrative »[1451] concernée. Mais si l'autorité en question refuse de le faire, la CADA ne dispose pas du pouvoir de poursuivre cette administration. Remarquons qu'à cet égard, la CPVP a plus de pouvoir. Lorsque les membres de la Commission procèdent à un examen sur place, ils ont la qualité de police judiciaire et peuvent exiger la communication de documents. En cas de mauvaise volonté de l'administration, la CPVP peut effectuer une dénonciation au Procureur du Roi ou saisir le tribunal de première instance.

Dans son rapport annuel de 2011, la CADA déplore cette absence de pouvoir décisionnel.

> Ainsi affirme-t-elle que « contrairement à la Commission d'accès aux et de réutilisation des documents administratifs, section Réutilisation, [...] la Commission d'accès aux et de réutilisation des documents administratifs, section Publicité de l'administration, n'a qu'une compétence d'avis et pas de compétence décisionnelle. La Commission ne perçoit pas pourquoi, sur le plan de la protection juridique, une distinction devrait être établie entre ces commissions. En ce qui concerne (le droit à) la réutilisation de documents administratifs qui – contrairement au droit à la publicité de l'administration (voir l'article 32 de la Constitution) – n'a pas le statut de droit fondamental et n'est pas reconnu comme un droit de l'homme par la Convention du Conseil de l'Europe sur l'accès aux documents officiels, il n'est certainement pas facile de comprendre pourquoi le citoyen jouit d'une protection juridique moindre en ce qui concerne l'accès aux documents administratifs »[1452].

[1450] Courrier du 7 juillet 2010.
[1451] Art. 19, §1, de l'arrêté royal du 29 avril 2008 précité.
[1452] Voy. le rapport annuel 2001, p. 22.

II. Le contrôle par les autorités juridictionnelles

432.- Considérations générales. Les litiges en lien avec l'e-gouvernement peuvent être portés devant les autorités juridictionnelles. Ces dernières sont compétentes pour imposer des sanctions contraignantes et prohibitives qui incitent au respect du régime juridique de la protection des données à caractère personnel.

> Par exemple, une loi contraire à l'article 22 de la Constitution peut être annulée par la Cour constitutionnelle, un tribunal peut condamner au paiement de dommages et intérêts la personne responsable d'un accès illégal à une base de données, etc.

Inversement, le contrôle effectué par les juridictions est affiné par les règles de protection des données à caractère personnel. Celles-ci offrent aux avocats et aux juges de nouveaux arguments pour contrôler le contenu des normes de valeur législative et réglementaire applicables à l'e-gouvernement, et sanctionner les utilisations abusives de données au sein de l'administration. Malheureusement, trop souvent encore, les arguments tirés du régime juridique de la protection des données à caractère personnel ne sont pas invoqués par les avocats ou le sont mal[1453].

Les développements qui suivent portent, d'une part, sur le contrôle de l'e-gouvernement par la Cour constitutionnelle et le Conseil d'État, section du contentieux administratif, et, d'autre part, sur le contrôle de l'e-gouvernement par les autorités juridictionnelles.

A. Le contrôle par la Cour constitutionnelle et le Conseil d'État

433.- Introduction. Tant l'encadrement normatif de l'e-gouvernement que les actes administratifs qui concrétisent des pratiques d'e-gouvernement sont soumis à un contrôle.

Des normes de valeur législative et des normes de valeur réglementaire encadrent l'e-gouvernement, comme l'a montré le premier titre de

[1453] Pour des exemples d'affaires dans lesquelles le régime juridique de la protection des données à caractère personnel n'a pas suffisamment été exploité, voy. not. Bruxelles (9e ch.), 9 mai 2012, *J.T.,* 2012, p. 691 et obs. E. Degrave, « La carte d'identité électronique utilisée comme carte de fidélité. : un traitement de données à caractère personnel illégal sanctionné par la Cour d'appel de Bruxelles » ; C.E., A.S.B.L. *Syndicat national des propriétaires et al.,* arrêt n° 216.928 du 19 décembre 2011 (voy. *infra,* n° 445.-). Pour des exemples d'affaires dans lesquelles ce régime juridique n'a pas été invoqué alors qu'il aurait pu l'être utilement, voy. not. C.C., arrêts n° 06/2013, du 14 février 2013 ; n° 18/2013, du 21 février 2013 ; n° 54/2013, du 18 avril 2013 ; n° 66/2013, du 16 mai 2013.

la recherche. La constitutionnalité des normes de valeur législative est contrôlée par la Cour constitutionnelle, tandis que l'examen de la constitutionnalité et de la légalité des normes de valeur réglementaire est de la compétence du Conseil d'État, section du contentieux administratif.

Par ailleurs, en pratique, l'e-gouvernement génère l'adoption d'actes administratifs dont la légalité est en principe[1454] contrôlée par le Conseil d'État, section du contentieux administratif[1455].

L'ensemble de ces contrôles forme le contentieux objectif. Les lignes qui suivent abordent successivement l'examen de constitutionnalité des normes de valeur législative qu'effectue la Cour constitutionnelle et l'examen de constitutionnalité et de légalité des normes de valeur réglementaire réalisé par le Conseil d'État.

§1. Le contrôle par la Cour constitutionnelle

434.- Présentation. La Cour constitutionnelle est instituée par la Constitution[1456] et organisée par une loi spéciale[1457]. Cette haute juridiction est compétente pour contrôler la constitutionnalité des normes de valeur législative[1458]. À ce titre, elle est appelée à se prononcer sur les lois, les décrets et les ordonnances qui encadrent l'e-gouvernement.

L'article 22 de la Constitution, interprété au regard du régime juridique de la protection des données, a pour effet d'élargir le contrôle que la Cour constitutionnelle effectue sur l'action de l'administration. En effet, des éléments qui relevaient jadis du pouvoir discrétionnaire des administrations doivent dorénavant être réglés par le législateur. Ce sont autant d'occasions, pour la Cour, de vérifier la constitutionnalité des développements de l'e-gouvernement.

Pour l'heure, la Cour constitutionnelle n'a pas encore été amenée à se prononcer sur la constitutionnalité d'une loi, d'un décret ou d'une ordonnance organisant une source authentique de données ou une plateforme d'échanges de données à disposition de l'administration, bien que certains de ces outils phares de l'e-gouvernement posent question au regard de

[1454] Sur le contrôle de la légalité des actes administratifs en matière de sécurité sociale et en matière fiscale, voy. *infra,* n°s 455.- et s.

[1455] Par exception à la compétence du Conseil d'État, certaines juridictions judiciaires sont compétentes pour annuler des actes administratifs déterminés. Elles sont étudiées dans la suite de la recherche. Voy. *infra,* n°s 450.- et s.

[1456] Voy. l'art. 142 de la Constitution.

[1457] Loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, *M.B.,* 7 janvier 1989.

[1458] Art. 1 de la loi spéciale du 6 janvier 1989 précitée.

l'article 22 de la Constitution, comme en attestent les problèmes constitutionnels soulevés par la section de législation du Conseil d'État[1459].

La Cour constitutionnelle a néanmoins été saisie de quelques normes qui organisent certains traitements de données. À cette occasion, elle livre des enseignements utiles pour l'étude de l'e-gouvernement, principalement s'agissant de l'interprétation de l'article 22 de la Constitution au regard des technologies de l'information et de la communication, comme cela fut déjà souligné à plusieurs reprises dans le premier titre de la recherche[1460].

1. Le contrôle des normes de valeur législative

435.- Un contrôle des lois, décrets et ordonnances. La Cour constitutionnelle peut être amenée à contrôler une loi, un décret ou une ordonnance qui fonde un traitement de données à caractère personnel. Ce faisant, elle examine la manière dont le législateur organise l'e-gouvernement.

Les conséquences d'un constat d'inconstitutionnalité sont importantes et varient selon que la Cour a été saisie d'un recours en annulation ou d'une question préjudicielle.

436.- Le recours en annulation. Un recours en annulation, éventuellement assorti d'une demande en suspension, peut être adressé à la Cour constitutionnelle à l'encontre des normes de valeur législative publiées depuis moins de six mois[1461]. Seuls les requérants limitativement énoncés par la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle peuvent introduire un tel recours.

> L'article 2 de la loi spéciale du 6 janvier 1989 énonce trois catégories de requérants et dispose que « Les recours visés à l'article 1er sont introduits :
>
> 1° par le Conseil des ministres, par l'exécutif d'une Communauté ou d'une Région ;
>
> 2° par toute personne physique ou morale justifiant d'un intérêt ; ou
>
> 3° par les présidents des assemblées législatives à la demande de deux tiers de leurs membres ».

[1459] Voy. *supra,* Titre I. Signalons que la Cour constitutionnelle pourrait être saisie prochainement d'un recours contre la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions, *M.B.,* 24 août 2012. Voy. http://www.lalibre.be/economie/actualite/article/757579/la-nouvelle-loi-sur-les-competences-du-fisc-bientot-attaquee.html

[1460] Voy. *supra,* nos 100.- et s.

[1461] Voy. les art. 1 à 25 de la loi spéciale du 6 janvier 1989 précitée.

Si le recours aboutit à l'annulation de la norme qui fonde le traitement de données, celui-ci ne pourra en principe[1462] plus être exécuté à l'avenir. En d'autres termes, l'annulation de la norme aboutit à l'anéantissement de l'entrepôt de données, de la source authentique de données, de la plateforme d'échanges d'informations, des échanges de données organisés par ladite norme. Ces traitements de données étant inconstitutionnels, l'administration ne peut plus les accomplir sous peine de commettre une illégalité constitutive d'une faute au sens de l'article 1382 du Code civil[1463]. Le législateur est alors contraint de revoir sa copie en veillant à respecter la Constitution.

437.- La question préjudicielle. Une juridiction peut saisir la Cour constitutionnelle d'une question préjudicielle. La question doit porter sur une norme de valeur législative que la juridiction est appelée à appliquer mais dont la constitutionnalité pose question, peu importe la date de publication de cette norme[1464].

Si la Cour constitutionnelle parvient à un constat d'inconstitutionnalité de la norme, le juge du fond qui a posé la question préjudicielle, ainsi que toute autre juridiction appelée à statuer dans la même affaire, doivent se conformer à la décision de la Cour constitutionnelle en n'appliquant pas la norme inconstitutionnelle au litige qui leur est soumis[1465]. Néanmoins, un tel constat retentit au-delà d'un litige en particulier. En effet, il ouvre un nouveau délai de six mois pour intenter un recours en annulation à l'encontre de la norme inconstitutionnelle[1466]. En outre, la décision de la Cour constitutionnelle peut faire jurisprudence car les juges amenés ultérieurement à connaître de la norme frappée d'inconstitutionnalité sont incités à ne plus l'appliquer.

Etant donné que le mécanisme de la question préjudicielle n'est pas soumis au respect d'un délai, des normes adoptées il y a des années peuvent être soumises à la Cour par cette voie. Une question préjudicielle peut ainsi être posée au sujet de lois adoptées avant l'ère de l'informatique, et qui pourtant constituent aujourd'hui le fondement légal de traitements de données importants, suscitant maintes interrogations en ce qui concerne notamment la prévisibilité des traitements organisés[1467].

[1462] En vertu de l'art. 8, al. 2, de la loi spéciale du 6 anvier 1989, la Cour pourrait néanmoins décider de maintenir, pendant un certain délai, les effets de la norme annulée (à ce sujet, voy. M. VERDUSSEN, *Justice constitutionnelle, op. cit.,* pp. 269 et 270).

[1463] Voy. *infra,* n° 456.-

[1464] Art. 26 à 30 de la loi spéciale du 6 janvier 1989 précitée.

[1465] *Ibid.,* art. 28.

[1466] *Ibid.,* art. 4.

[1467] Voy. *supra* Titre I.

La Cour pourrait alors déclarer la législation inconstitutionnelle au regard de l'article 22 de la Constitution en raison du fait, notamment, que les éléments essentiels du traitement de données n'y sont pas définis. Le législateur serait invité à se mettre en ordre. Ce faisant, l'arsenal législatif de notre pays serait progressivement adapté à l'ère de l'e-gouvernement.

> On pense, par exemple, à la loi du 16 novembre 1972 concernant l'inspection du travail dont il a déjà été question[1468]. Cette loi constitue le fondement légal de la communication de données vers le *datawarehouse* OASIS servant à lutter contre la fraude sociale, alors que cette loi organise un équilibre entre les prérogatives des inspecteurs sociaux et les droits des citoyens qui ne tient pas compte des outils informatiques puisque ceux-ci n'existaient pas encore. Si le législateur souhaite que cette loi constitue le fondement de l'utilisation d'OASIS, il doit la réexaminer et organiser explicitement l'utilisation de ce *datawarehouse* en mentionnant sa finalité, les données enregistrées, les responsabilités qu'il induit et les garanties à offrir aux personnes concernées, en termes de transparence notamment.

2. Le contrôle au regard des libertés fondamentales et des règles répartitrices de compétences

438.- Les normes de référence. L'examen opéré par la Cour constitutionnelle permet d'étudier la constitutionnalité d'un traitement de données sous différents angles. Ainsi, non seulement la Cour constitutionnelle est-elle habilitée à vérifier que ledit traitement de données ne porte pas atteinte à l'article 22 de la Constitution, mais elle peut également le confronter aux autres droits fondamentaux consacrés par le Titre II de la Constitution « Des belges et de leurs droits » ainsi qu'aux articles 170, 172 et 191 de la Constitution.

Ce contrôle constitutionnel permet également de sanctionner les normes organisant un traitement de données qui violent les règles répartitrices de compétences entre la collectivité fédérale, les communautés et les régions établies par la Constitution ou en vertu de celle-ci.

439.- Les droits fondamentaux. La Cour constitutionnelle contrôle les normes organisant des traitements de données au regard de l'article 22 de la Constitution, qui protège la protection de la vie privée, mais également au regard des autres droits fondamentaux consacrées par le Titre II de la Constitution.

[1468] Voy. *supra,* n° 133.-

a) L'article 22 de la Constitution. Rappelons qu'après quelques tergiversations[1469], la Cour constitutionnelle applique aujourd'hui la méthode du « tout indissociable » et contrôle les normes organisant un traitement de données à caractère personnel par rapport à l'article 22 de la Constitution, interprété au regard de l'article 8 de la Convention européenne des droits de l'homme, de la Convention n° 108 et de la directive 95/46. Cela permet d'enrichir l'article 22 de la Constitution des exigences de la protection des données et de l'interprétation qui en est donnée par les juridictions supra nationales.

b) Les autres libertés fondamentales. Un traitement de données à caractère personnel est susceptible de porter atteinte à d'autres droits fondamentaux. C'est pour cette raison d'ailleurs que d'aucuns soutiennent à juste titre que le droit à la protection de la vie privée est la condition de réalisation des autres droits fondamentaux[1470] et que la loi du 8 décembre 1992 prévoit en son article 2 que « lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée ».

Etant compétente pour contrôler les normes au regard de l'ensemble du Titre II, la Cour constitutionnelle peut également examiner les développements de l'e-gouvernement à la lumière d'autres droits fondamentaux consacrés par la Constitution, telles que les exigences d'égalité et de non-discrimination, la liberté d'expression, le droit de propriété, etc. De plus, l'application de la « méthode combinatoire » permet à la Cour constitutionnelle d'intégrer « des normes internationales dans le contrôle d'égalité ; elle considère ainsi qu'une atteinte discriminatoire à un droit international peut être constitutive d'une violation des articles 10 et 11 de la Constitution, sièges du principe d'égalité et de non discrimination »[1471].

À cet égard, nous avons souligné dans le prélude de cette recherche que les règles de protection des données permettent de protéger la vie privée mais également d'autres droits fondamentaux.

[1469] Voy., *supra,* n°s 101.- et s.

[1470] H. Burkert, « Dualities of Privacy – An Introduction to 'personal Data protection and Fundmental Rights », *in* M.V. Perez, A. Palazzi et Y. Poullet (dir.), *Privacy-New visions,* Cahier du Crid, n° 31, 2008, pp. 13 à 23 ; Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in État de droit et virtualité* (éd. K. Benyekhlef et P. Trudel), Montréal, Thémis, 2009, pp. 177.

[1471] M. Verdussen, *Justice constitutionnelle, op. cit.,* p. 126.

> Par exemple, en encadrant l'utilisation des données relatives à l'appartenance syndicale, on protège la liberté d'association ; en limitant l'usage des données relatives à l'appartenance religieuse, on encourage la liberté de culte, etc.[1472]

440.- Les règles répartitrices des compétences. Comme on l'a souligné précédemment, la collectivité fédérale, les communautés et les régions peuvent chacune régler les traitements de données nécessaires à l'accomplissement des compétences qui sont les leurs. Néanmoins, compte tenu du fait que la circulation des données s'étend bien souvent au-delà des frontières d'une entité, il y a un risque qu'en réglant ces questions, le législateur fédéral empiète sur les compétences communautaires ou régionales, et inversement.

Il y aurait alors une atteinte à l'exclusivité des compétences qui fonde l'organisation fédérale de notre pays et, dès lors, une violation des règles répartitrices de compétence dont la Cour constitutionnelle peut connaître. Le principe de proportionnalité dans l'exercice des compétences pourrait également être atteint[1473].

> Par exemple, un décret régional réglant la perception des redevances de stationnement dans les communes ne pourrait imposer au législateur fédéral de communiquer aux communes les données d'identification des conducteurs en défaut de paiement. En imposant une obligation nouvelle à l'entité fédérale, la Région porterait atteinte notamment à l'exclusivité des compétences de chaque entité[1474].

Face à cette problématique, il revient à la Cour constitutionnelle de veiller à ce que les lois, décrets et ordonnances organisant des traitements de données dans l'administration respectent les règles répartitrices de compétences ainsi que le principe de proportionnalité dans l'exercice des compétences. À cette occasion, elle peut inciter les autorités concernées à conclure un accord de coopération. Elle le fait, par exemple, en annulant la législation attaquée tout en maintenant les effets de celle-ci durant un certain délai, afin de permettre aux législateurs concernés de conclure un accord de coopération.

> Dans un arrêt mentionné précédemment qui concerne l'encadrement législatif des communications électroniques[1475], la Cour constitutionnelle souligne notamment que « les compétences de l'État fédéral et des communautés en

[1472] Voy. *supra,* n° 64.-
[1473] Voy. *supra,* n° 227.-
[1474] Pour un cas semblable, voy. *infra*, dans ce même point.
[1475] Voy. *supra,* n° 228.-

> matière d'infrastructure des communications électroniques sont devenues à ce point imbriquées, par suite de l'évolution technologique, qu'elles ne peuvent plus être exercées qu'en coopération »[1476]. Elle annule la loi attaquée par le Gouvernement flamand, mais maintient les effets de la loi annulée durant cinq mois, le temps pour le législateur fédéral et le législateur flamand, d'adopter « une réglementation prise de commun accord »[1477].

Récemment, la Cour constitutionnelle a eu une belle occasion d'encourager l'adoption d'un accord de coopération concernant l'e-gouvernement. Malheureusement, elle a manqué de s'en saisir. L'arrêt rendu laisse perplexe[1478].

Nous avons évoqué cette affaire en guise d'exemple dans les lignes qui précèdent. Un décret flamand règle notamment la perception des redevances de stationnement en prévoyant que les communes peuvent demander à l'administration fédérale chargée de l'immatriculation des véhicules (DIV) les données du registre qu'elle détient et qui permettent d'identifier le titulaire d'une plaque d'immatriculation en défaut de paiement. Le Conseil des ministres conteste ce décret, arguant du fait qu'un décret ne peut imposer unilatéralement à la collectivité fédérale de communiquer les informations d'identification issues du registre de la DIV, étant donné que cela violerait l'exclusivité des compétences. Le Gouvernement flamand répond que le décret prévoit seulement que les communes peuvent demander les informations à la DIV, qui reste libre de les donner ou pas, tout en ajoutant que si elle refuse de les donner, sans motif légitime, elle viole la loyauté fédérale et le principe de la proportionnalité dans l'exercice des compétences[1479].

Face à ce conflit, la Cour constitutionnelle rend un arrêt décevant. Elle esquive l'argument de l'atteinte à l'exclusivité des compétences. Elle se contente de dire que la finalité de l'accès aux données d'identification, telle que décrite par le décret flamand, correspond à la finalité de communication des données DIV définie par l'arrêté royal du 20 juillet 2001 qui organise le registre de la DIV. Elle écarte le moyen invoqué par

---

[1476] C. C., arrêt n° 132/2004, du 14 juillet 2004, concernant le recours en annulation de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges, la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information visés à l'article 77 de la Constitution, la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *in*troduit par le Gouvernement flamand, B.6.2.

[1477] *Ibid.,* B. 7.1.

[1478] C.C., arrêt n° 2/2012 du 11 janvier 2012.

[1479] *Ibid.,* A. 7.1.1. à A. 7.3.4.

le Conseil des ministres[1480] et rejette le recours. Le décret attaqué n'est pas annulé.

Ce raisonnement souffre de deux défauts majeurs.

Premièrement, la Cour juge la constitutionnalité du décret flamand au regard d'un arrêté royal, ce qui est particulièrement contestable au regard de la hiérarchie des normes dans l'État fédéral et de l'article 1 de la loi spéciale du 6 janvier 1989 qui impose de confronter les normes attaquées à la Constitution.

Deuxièmement, la Cour méconnaît les exigences cardinales du régime de la protection des données à caractère personnel. En effet, elle constate que la finalité d'accès aux données prévue par le décret flamand correspond à la finalité de communication des données déterminée par l'arrêté royal organisant la DIV. À partir de là, elle en conclut que la communication des données de la DIV vers les communes flamandes est légale. La Cour semble oublier que la finalité n'est qu'une exigence parmi bien d'autres et qu'il s'impose également de vérifier la proportionnalité du traitement, la proportionnalité des données utilisées, la base légale dans le chef de l'autorité qui communique et de celle qui reçoit les informations.

Il aurait été plus rigoureux de décider qu'en ce que le décret flamand n'impose pas à la collectivité fédérale de communiquer les informations de la DIV aux communes flamandes, mais prévoit seulement que les communes peuvent introduire une demande d'accès aux données de la collectivité fédérale, ledit décret ne viole pas l'exclusivité des compétences. Un tel raisonnement, même s'il aboutit au même résultat que dans cet arrêt, aurait paru plus orthodoxe. La Cour aurait dû ajouter que, néanmoins, compte tenu de l'importance d'une collaboration entre la collectivité fédérale et les régions pour identifier, via une banque de données informatisée, les citoyens en défaut de payer la redevance de stationnement qui leur a été imposée, il s'impose de conclure un accord de coopération. La Cour aurait pu annuler le décret flamand en suspendant ses effets de quelques mois, le temps pour le législateur fédéral et le législateur décrétal, de s'accorder sur une réglementation en ce domaine.

§2. Le contrôle par le Conseil d'État

441.- Introduction. Comme on l'a constaté pour la Cour constitutionnelle, le régime de la protection des données à caractère personnel affine

[1480] *Ibid.,* B. 12.3.2. à B.1.3.

également le contrôle que le Conseil d'État, section du contentieux administratif[1481], exerce sur l'action administrative.

> Ainsi, par exemple, un échange d'informations, qui constituait jadis une simple mesure préparatoire d'une décision administrative et relevait du pouvoir discrétionnaire des administrations, doit aujourd'hui respecter les exigences légales et constitutionnelles qui protègent les données à caractère personnel des administrés. Un échange de données abusif peut ainsi justifier l'annulation d'un acte administratif.

1. Le contrôle des actes administratifs

442.- Les actes administratifs contrôlés. En vertu de l'article 14, §1, des Lois coordonnées sur le Conseil d'État, le Conseil d'État est en principe[1482] compétent pour connaître des recours introduits contre les actes administratifs, à portée règlementaire ou individuelle[1483].

Le Conseil d'État peut ainsi connaître d'actes administratifs dont la légalité suppose le respect du régime juridique de la protection des données à caractère personnel.

> Entre autres exemples, on pense à une décision administrative fondée sur un traitement de données à caractère personnel ou un arrêté royal exécutant une loi qui organise un tel traitement.

En outre, depuis une modification des lois coordonnées sur le Conseil d'État intervenue en 1999[1484], « les décisions des assemblées législatives ou de leurs organes, en ce compris les médiateurs institués auprès de ces assemblées, de la Cour des comptes et de la Cour constitutionnelle, du Conseil d'État et des juridictions administratives ainsi que des organes du pouvoir judiciaire et du Conseil supérieur de la Justice »[1485] peuvent également faire l'objet d'un recours devant le Conseil d'État, mais uniquement lorsqu'elles sont relatives aux marchés publics et aux membres de leur personnel.

[1481] Pour faciliter la lecture de ce deuxième paragraphe, nous utilisons les termes « Conseil d'État » pour désigner la section du contentieux administratif du Conseil d'État.

[1482] Précisons que le Conseil d'État est incompétent pour connaître des actes administratifs pris en matière de sécurité sociale et en matière fiscale. À ce sujet, voy. *infra,* n° 455.-

[1483] Nous n'analysons pas, dans cette recherche, la compétence du Conseil d'État pour connaître des décisions d'une juridiction administrative.

[1484] Loi du 25 mai 1999 modifiant les lois sur le Conseil d'État, coordonnées le 12 janvier 1973, la loi du 5 avril 1955 relative aux traitements des titulaires d'une fonction au Conseil d'État, ainsi que le Code judiciaire, *M.B.,* 22 juin 1999.

[1485] Art. 14, 2°, des lois coordonnées sur le Conseil d'État.

Ces actes administratifs peuvent être attaqués au Conseil d'État par un recours en annulation, éventuellement assortis d'un recours en suspension[1486]. Le recours doit être intenté dans un délai de 60 jours à partir du moment où l'acte a été publié, notifié ou porté à la connaissance des intéressés[1487].

443.- Un contrôle limité de l'e-gouvernement. On l'a dit, le Conseil d'État ne peut connaître que des actes administratifs unilatéraux, de portée règlementaire ou individuelle.

Cette limitation de compétence empêche d'intenter un recours au Conseil d'État contre les nombreux transferts de données entre administrations qui fondent l'e-gouvernement. En effet, la décision d'une administration de transférer des données à une autre institution, n'est pas, en elle-même, source de grief pour l'administré. Elle est une mesure préparatoire d'une décision administrative qui, elle, constitue un acte administratif susceptible d'un recours devant le Conseil d'État[1488]. Cela signifie que, même si un citoyen a connaissance d'un transfert illégal de ses données au sein de l'administration, il ne peut pas le contester devant le Conseil d'État. Il doit attendre que lui soit notifiée la décision administrative fondée sur un tel traitement de ses données et ensuite attaquer cette décision fondée sur des motifs illégaux[1489].

Par ailleurs, le Conseil d'État ne peut qu'annuler l'acte attaqué sans pouvoir imposer à l'administration qu'elle reprenne un acte conforme aux lois[1490]. Ainsi, l'annulation d'une décision administrative fondée sur des données inexactes ou des données que l'administration ne peut utiliser pour l'accomplissement de ses missions, n'emporte en principe pas l'obligation, pour ladite administration, de reprendre une décision à partir des données exactes ou légalement obtenues.

[1486] *Ibid.,* art. 14, 17 et 19.

[1487] Art. 4 de l'arrêté du Régent du 23 août 1948 déterminant la procédure devant la section du contentieux administratif du Conseil d'État.

[1488] R. Andersen et P. Lewalle, « La motivation formelle des actes administratifs », *A.P.T.*, 1993, p. 67 ; J. Salmon, *Le Conseil d'État,* T. I, Bruxelles, Bruylant, 1994, p. 274 ; P. Lewalle, *Contentieux administratif, op. cit.,* pp. 248 à 250 ; I. Opdebeek et A. Coolsaet, *Formele motivering van bestuurshandelingen*, Brugge, die Keure, 1999, pp. 168-169 ; M. Maerevoet, *La motivation formelle des actes administratifs en matière de marchés publics*, Bruxelles, Larcier, 2011, p. 65. À ce sujet, voy. *supra*, Titre II, Chapitre 1, Section 3.

[1489] Voy. *infra,* n° 444.-, 445.- et s.

[1490] Néanmoins, dans certaines hypothèses, la réfection de l'acte est obligatoire, cette obligation étant imposée par la loi et non le Conseil d'État. À ce sujet., voy. not., D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *Droit administratif. Tome III. Le contrôle de l'administration,* Bruxelles, Larcier, 2010, p. 298.

2. Les motifs du contrôle

444.- Le respect des normes de valeur supérieure. Les actes administratifs relatifs à l'e-gouvernement sont soumis à un contrôle étendu du Conseil d'État qui peut les examiner au regard de l'ensemble des normes hiérarchiquement supérieures, c'est-à-dire les normes de valeur législative, la Constitution et le droit supranational.

Le Conseil d'État est susceptible d'annuler l'acte attaqué dans trois hypothèses, à savoir, la violation des formes substantielles ou prescrites à peine de nullité, l'excès de pouvoir (incompétence de l'auteur de l'acte ou violation d'une règle de droit), et le détournement de pouvoir[1491].

445.- L'apport du régime juridique de la protection des données à caractère personnel. On a montré, dans le premier titre de cette recherche consacré à l'exigence de légalité, que les règles de protection des données confortent, et même renforcent, le droit administratif. En toute logique, ce phénomène se manifeste également dans le contrôle opéré par le Conseil d'État sur les actes de l'administration.

Ainsi, on constate que tantôt l'application du régime juridique de la protection des données à caractère personnel aboutit à une solution semblable à celle imposée par des normes de droit administratif appliquées par le Conseil d'État, telles que la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs. En ce sens, la protection des données à caractère personnel conforte le contrôle du Conseil d'État. Tantôt l'application du régime juridique de la protection des données à caractère personnel permet un contrôle plus sévère de l'action administrative. À cet égard, la protection des données à caractère personnel renforce le contrôle du Conseil d'État.

Un arrêt récent montre l'intérêt de recourir au régime juridique de la protection des données lors d'un recours intenté au Conseil d'État. Il illustre également le fait que ce régime juridique particulier est encore trop peu connu des administrativistes.

> Dans cette affaire, le Syndicat national des propriétaires, ainsi que d'autres requérants, intentent un recours en annulation au Conseil d'État à l'encontre d'un arrêté de Gouvernement portant exécution du Code bruxellois du Logement[1492]. Les requérants critiquent notamment le fait que cet arrêté institue un droit de gestion publique dans le chef d'opérateurs immobi-

[1491] Art. 14 des lois coordonnées sur le Conseil d'État.

[1492] C.E., A.S.B.L. *Syndicat national des propriétaires et al.*, arrêt n° 216.928 du 19 décembre 2011.

> liers publics, qui porte sur certains logements, parmi lesquels figurent les « logements inoccupés ». Pour considérer que le logement est inoccupé, il faut notamment se référer à un seuil de consommation d'eau et un seuil de consommation d'électricité, fixés par ledit arrêté de Gouvernement.
>
> Les requérants soutiennent notamment que ces informations sont des données à caractère personnel et critiquent le fait que l'acte attaqué ne précise pas « les conditions dans lesquelles ces informations peuvent être délivrées » et n'indique pas « les garanties suivant lesquelles elles pourraient l'être »[1493]. Malheureusement, les requérants n'étayent pas leur argumentation. En particulier, ils n'invoquent pas la loi du 8 décembre 1992 et ne précisent pas quelles dispositions légales sont violées par l'acte attaqué.
>
> Dès lors, le Conseil d'État répond que le moyen « ne vise [...] pas les dispositions ou principes qui, à l'estime des requérantes, seraient violés, ni en quoi ils l'auraient été. Il s'ensuit que, sans qu'il s'agisse de faire preuve d'un formalisme excessif, le moyen doit être déclaré irrecevable en tant qu'il prend appui sur ce grief »[1494].
>
> Dans cette affaire, les règles de protection des données ont donc été approchées, mais pas suffisamment exploitées. Les requérants auraient pu notamment invoquer des arguments tirés de l'exigence de finalité du traitement (Est-elle suffisamment précise ? Est-elle légitime ?). L'exigence de compatibilité entre la finalité de la collecte des données et celle de leur réutilisation aurait également pu être étudiée, tout comme la proportionnalité des données et de ce traitement. Les requérants auraient pu également s'interroger sur la nécessité d'obtenir une autorisation de comité sectoriel avant de traiter pareilles données, etc.

Les lignes qui suivent illustrent le fait que le régime juridique de la protection des données conforte et renforce le droit administratif, à partir de certains cas qui ont été soumis au Conseil d'État, ou qui pourraient l'être.

a) Le contrôle du Conseil d'État conforté par la protection des données

446.- L'indisponibilité des compétences et l'interdiction de décisions automatisées. Certaines matières juridiques sont si complexes que l'autorité administrative peut éprouver le besoin de recourir à un outil informatique d'aide à la décision.

> Par exemple, le Conseil d'État a déjà été saisi de plusieurs recours concernant l'utilisation d'un outil informatique dans le cadre de l'attribution d'un marché public. Il est reproché à l'autorité administrative de ne pouvoir

[1493] *Ibid.,* p. 19.
[1494] *Ibid.,* p. 22.

> expliquer son choix, trop largement dicté par les calculs opérés par l'ordinateur[1495].
>
> Une critique semblable peut également être formulée à l'égard de l'utilisation, par les services d'inspection sociale, de l'entrepôt de donnés OASIS pour identifier les fraudeurs potentiels. Les algorithmes mathématiques utilisés par cet outil informatique sont si compliqués qu'un humain ne peut en comprendre la logique.

Dans pareille hypothèse, le Conseil d'État est compétent pour vérifier que l'autorité administrative a exécuté elle-même les missions qui lui sont légalement attribuées, en exerçant effectivement son pouvoir d'appréciation. Le fait de donner un pouvoir de décision à un ordinateur – en le laissant choisir un soumissionnaire dans le cadre d'un marché public ou en imposant une sanction liée à une fraude sociale sans avoir effectué une inspection sur place, pour reprendre les exemples ci-dessus – serait contraire au principe de l'indisponibilité des compétences consacré par l'article 33 de la Constitution. Elle s'apparenterait à une délégation de compétence à un outil informatique, tel qu'un ordinateur ou l'entrepôt de données OASIS.

Saisi d'un recours contre un acte fondé sur un traitement de données à caractère personnel, le Conseil d'État pourrait aboutir à la même solution en appliquant l'article 12*bis* de la loi du 8 décembre 1992 qui interdit les décisions entièrement automatisées.

> L'article 12*bis* de la loi du 8 décembre 1992 dispose qu' « une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité.
>
> Cette interdiction ne s'applique pas « lorsque la décision [...] est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance ». Néanmoins, la loi du 8 décembre 1992 ajoute que, dans ce cas, ladite disposition doit « contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue ».
>
> Pour reprendre les exemples précédents, l'attribution d'un marché public ne pourrait résulter de la seule décision d'un ordinateur. Le pouvoir adjudicateur doit procéder lui-même à une évaluation des offres et être en mesure de justifier son choix. Dans le même sens, une personne coupable de fraude en matière sociale ne peut être sanctionnée sur la seule base de son

[1495] Voy. not. C.E., 16 septembre 2004, *Computer Sciences,* n° 134.986 ; C.E., 7 mars 2006, *SA Construction industrielles de la méditerranée et alii*, n° 155.931 ; C.E., 8 juin 2006, *NV EurosenseBelfotop,* n° 159.782 ; C.E., 27 décembre 2006, *N.V. Bioterra et alii,* n° 166.318.

identification par le système OASIS. L'intervention d'un inspecteur social qui effectue un réel contrôle sur place est nécessaire.

447.- La motivation formelle des actes administratifs et la qualité des données à caractère personnel. Il existe un lien entre la loi sur la motivation formelle des actes administratifs et la qualité des données à caractère personnel utilisées. En effet, si la donnée utilisée dans le cadre d'une décision administrative est fausse, elle ne correspond pas à la réalité. De ce fait, on doit considérer que la motivation de cette décision n'est pas « adéquate », au sens de l'article 3 de la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs[1496].

Dans pareille hypothèse, le Conseil d'État pourrait également appliquer la loi du 8 décembre 1992 qui exige le traitement des données exactes et à jour. L'acte administratif fondé sur des données erronées ne respecte pas l'article 4, 3°, de la loi du 8 décembre 1992. Il est illégal et doit donc être annulé.

b) Le contrôle du Conseil d'État renforcé par la protection des données

448.- Le contrôle des moyens utilisés par l'administration en amont des décisions administratives. En veillant au respect de la loi du 8 décembre 1992, le Conseil d'État étend son contrôle aux « coulisses » des décisions administratives. En effet, avant l'instauration du régime de la protection des données, les actes préparatoires aux décisions administratives – tels que le transfert des données des citoyens – relevaient en principe du pouvoir discrétionnaire des administrations. Le Conseil d'État jugeait de la légalité des décisions finales, mais ne pouvait contrôler l'utilisation des données à caractère personnel des citoyens étant intervenue en amont de celles-ci, puisque nulle obligation légale ne s'y appliquait.

Par exemple, quand une administration avait besoin d'une information relative à un citoyen, elle interrogeait directement ce dernier ou demandait à une institution voisine de lui communiquer par voie postale la photocopie du document recherché.

Aujourd'hui, les règles relatives à la protection des données à caractère personnel imposent de nouvelles obligations aux administrations, y compris au stade des mesures préparatoires des actes administratifs. Ces règles restreignent le pouvoir des administrations de choisir discrétionnairement les moyens qu'elles utilisent pour accomplir leurs missions légales.

[1496] D. Lagasse, « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs », *J.T.*, 1991, p. 738.

En effet, une administration qui a besoin d'une information ne peut automatiquement se tourner vers le citoyen concerné ou l'institution qui la détient. Elle doit respecter le prescrit du régime de la protection des données à caractère personnel. Si l'auteur de l'acte ne respecte pas ces règles de droit, il commet un excès de pouvoir. L'acte est illégal et risque d'être annulé.

Plus particulièrement, le Conseil d'État pourrait ainsi annuler un acte administratif dont les mesures préparatoires violent les *conditions de fond* d'un traitement de données à caractère personnel imposées par la loi applicable. Tel est le cas si les données utilisées ne sont pas exactes ou ne respectent pas l'exigence de proportionnalité. Il en va de même pour l'administration qui ne respecterait pas l'obligation de collecte indirecte des données à laquelle elle serait soumise. En effet, l'institution rendrait une décision illégale si elle refusait l'octroi d'un droit au citoyen au motif qu'il n'a pas fourni le renseignement requis, alors qu'elle a le devoir de le trouver par elle-même via une collecte indirecte.

Les administrations sont également tenues au respect de *formalités* propres au régime de la protection des données à caractère personnel. Ces formalités, imposées par la loi du 8 décembre 1992, doivent obligatoirement être respectées. Un acte administratif qui les méconnaît serait illégal et, partant, pourrait être annulé par le Conseil d'État.

> Parmi ces formalités, on pense notamment à l'obligation pour une administration d'obtenir l'autorisation du comité sectoriel compétent en cas de collecte indirecte de données (article 31*bis* de la loi du 8 décembre 1992)[1497]. On pense également à l'obligation d'information des personnes concernées par un traitement de données (article 9 de la loi du 8 décembre 1992)[1498].

449.- Le contrôle des délégations de compétence au pouvoir exécutif. Comme rappelé dans le premier titre, l'article 108 de la Constitution s'oppose à ce que le Roi définisse les éléments essentiels d'une législation, à moins d'être encadré par des critères légaux.

L'article 22 de la Constitution, enrichi des normes supranationales qui organisent la protection des données à caractère personnel, guide le Conseil d'État sur l'identification des éléments d'un traitement de données qui doivent être organisés par le législateur et ceux qui peuvent être délégués au Roi dans le cadre de son pouvoir d'exécuter les lois[1499].

[1497] Sur cette obligation, voy. *infra*, n° 534.-

[1498] Sur cette obligation, voy. *supra* n° 353.-

[1499] Voy. *supra,* n° 102.- et s.

Se fondant sur ces normes, la section de législation du Conseil d'État a déjà critiqué plusieurs délégations de compétence, les jugeant contraires à l'article 108 de la Constitution[1500]. Certaines de ces dispositions critiquées ont néanmoins été adoptées[1501].

B. Le contrôle par les juridictions judiciaires

450.- Les articles 144 et 145 de la Constitution. En vertu des articles 144 et 145 de la Constitution, un citoyen peut saisir les juridictions judiciaires s'il estime que l'administration a violé un de ses droits subjectifs, de nature civile ou politique.

> En vertu de l'article 144 de la Constitution, « les contestations qui ont pour objet des droits civils sont exclusivement du ressort des tribunaux » tandis que l'article 145 de la Constitution prévoit que « les contestations qui ont pour objet des droits politiques sont du ressort des tribunaux, sauf les exceptions établies par la loi ».
>
> Par exemple, en vertu de l'article 144 de la Constitution, les juridictions judiciaires, au titre de leurs compétences générales, peuvent connaître des litiges mettant en cause la responsabilité civile extracontractuelle de l'administration.
>
> En vertu de l'article 145 de la Constitution et de l'article 580, 8°, du Code judiciaire, le tribunal du travail est compétent pour connaître des litiges relatifs au droit à l'intégration sociale.

Devant le juge judiciaire, trois voies d'action protègent le citoyen contre l'arbitraire de l'administration[1502] : la non-applicabilité de l'acte administratif illégal, en vertu de l'article 159 de la Constitution[1503] ; la

---

[1500] Voy. avis L. 33.962/2 du 19 novembre 2002 sur un avant-projet de loi « modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques », *op. cit.*, pp. 57-58 ; avis du 27 avril 1989 sur un projet de loi « instituant une Banque-Carrefour de la sécurité sociale », *op.cit.*, pp. 101 et 102 ; avis L. 33.285/1 du 2 mai 2002 sur un avant-projet de loi « portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce et création des guichets d'entreprises », *Doc. Parl.,* Chambre, session 2002-2003, n° 50-2058/001, p. 103.

[1501] Voy. not. l'article 15 de la loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.,* 22 février 1990.

[1502] Cette présentation des recours s'inspire des conclusions de M. l'avocat général Leclerq relative à l'arrêt de la Cour de cassation du 10 juin 1996, *R.C.J.B.,* 1997, pp. 449 à 453.

[1503] L'article 159 de la Constitution peut également être invoqué devant la section du contentieux administratif du Conseil d'État. Par souci de clarté, les développements relatifs à cette disposition sont regroupés dans le présent chapitre.

contestation directe, par l'administré, d'actes administratifs adoptés dans certaines matières et l'action en responsabilité civile de l'administration, en vertu de l'article 1382 du Code civil. Ces différentes protections sont à présent successivement confrontées à l'e-gouvernement.

§1. La non-applicabilité de l'acte administratif illégal

451.- L'article 159 de la Constitution. L'article 159 de la Constitution dispose que « les cours et tribunaux n'appliqueront les arrêtés et règlements généraux, provinciaux et locaux, qu'autant qu'ils sont conformes aux lois ». Il faut comprendre par là que le juge saisi d'un litige est tenu de ne pas appliquer les actes administratifs unilatéraux qui régissent une situation s'ils sont contraires à une norme hiérarchiquement supérieure.

La doctrine ne manque pas de souligner l'importance de cette disposition constitutionnelle qui, « constitue le plus ancien mode de protection juridictionnelle du citoyen face à l'arbitraire administratif et ouvre la plus ancienne voie dans laquelle le contrôle juridictionnel trouve à s'engager »[1504]. « En tout temps, [elle] permet au citoyen de solliciter la protection du juge face à l'action de l'administration »[1505]. L'article 159 de la Constitution consacre ainsi « un véritable droit de résistance au citoyen lorsqu'il est confronté à un acte illégal »[1506].

Les actes administratifs fondés sur un traitement de données à caractère personnel illégal peuvent être sanctionnés en vertu de l'article 159 de la Constitution, comme le soulignent les lignes qui suivent consacrées aux traits saillants du contrôle de légalité incident.

452.- L'auteur du contrôle. Seules les juridictions peuvent effectuer le contrôle de légalité organisé par l'article 159 de la Constitution. Une

---

[1504] D. De Roy, « L'exception d'illégalité instituée par l'article 159 de la Constitution : de la vision d'apocalypse à la juste mesure ? », note sous Cass. 16 juin 2006 et Cass. 23 octobre 2006, *R.C.J.B.,* 2009, p. 21.

[1505] D. Renders, « L'article 159 de la Constitution », *in La Constitution belge. Lignes et entrelignes* (dir. M. Verdussen), Bruxelles, Le Cri, 2003, p. 353.

[1506] M. Nihoul, « Introduction », *in L'article 159 de la Constitution. Le contrôle de légalité incident, op. cit.,* p. 15. Sur l'article 159 de la Constitution, voy. égal. not. J. Theunis, « De 'exceptie van onwettigheid' (artikel 159 G.W.) : meer vragen dan antwoorden ? », *R.W.,* 2007-2008, pp. 1266 à 1281 ; A. Mast, J. Dujardin, M. Van Damme et J. Vande Lanotte, *Overzicht van het Belgisch Administratief Recht,* 18e éd., Malines, Kluwer, 2009, pp. 863 à 890 ; D. Batsele, T. Mortier et M. Scarcez, *Manuel de droit administratif,* Bruxelles, Bruylant, 2010, pp. 715 à 718.

administration ne pourrait refuser d'appliquer un acte réglementaire au motif qu'il est irrégulier[1507].

Il faut néanmoins apporter une exception à ce principe, qui découle de l'obligation, pour un fonctionnaire, de refuser d'obéir à l'ordre hiérarchique manifestement illégal[1508]. Appliquée à l'administration, cette règle aboutit à considérer qu'une administration peut refuser d'appliquer un acte administratif unilatéral qui serait « manifestement » irrégulier[1509].

> Par exemple, une administration est qualifiée d'institution de sécurité sociale par un arrêté royal. Elle est, de ce fait, intégrée au réseau de la sécurité sociale et tenue de se soumettre à l'ensemble des obligations prévues par la loi du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale. Cette administration pourrait-elle refuser de se conformer à l'arrêté royal organisant son intégration dans ce réseau sectoriel au motif qu'il est irrégulier, ayant été élaboré par le Roi dans le cadre d'une délégation de compétence inconstitutionnelle, qui viole les articles 22 et 108 de la Constitution ? À notre sens la négative semble devoir prévaloir. On peut difficilement admettre une illégalité manifeste dans un tel cas. C'est probablement la raison pour laquelle de tels arrêtés royaux existent et subsistent[1510].

453.- Le contenu du contrôle. En principe[1511], seuls les actes administratifs unilatéraux de portée réglementaire ou individuelle peuvent faire l'objet d'un contrôle incident[1512].

Tout comme le contrôle de légalité effectué par la section du contentieux administratif du Conseil d'État dans le cadre d'un recours en annulation ou en suspension, le contrôle de légalité incident susceptible d'être

---

[1507] À ce sujet, voy. R. Van Melsen, « Le champ d'application personnel du contrôle de légalité incident », *in L'article 159 de la Constitution. Le contrôle de légalité incident, op. cit.,* pp. 23 et s. Néanmoins, l'auteur plaide pour la reconnaissance de la possibilité, pour les autorités administratives, d'effectuer elles-mêmes un contrôle de légalité. « Cette prérogative, difficilement évitable en pratique, [...] paraît devoir être fondée, du moins en l'état actuel du droit, sur un principe général de légalité dont l'article 159 est une application particulière » [*Ibid.,* p. 65].

[1508] Certaines normes consacrent explicitement cette obligation (voy. par exemple, l'article 8 de la loi portant le statut disciplinaire des membres du personnel des services de police, *M.B.,* 16 juin 1999). Cette règle est également un principe général de droit.

[1509] D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.*, p. 399 et les références citées.

[1510] Il s'agit principalement des arrêtés royaux qui étendent le réseau de la sécurité sociale en vertu de l'article 18 de la loi du 15 janvier 1990. Voy. *supra,* n° 122.-

[1511] Voy. l'art. 9 de la loi spéciale du 12 janvier 1989 relatives aux institutions bruxelloises.

[1512] Voy. not. D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.,* pp. 400 et s. ; F. Barcena, « Le champ d'application normatif du contrôle de légalité », *in L'article 159 de la Constitution. Le contrôle de légalité incident, op. cit.,* pp. 103 et s.

effectué par toute juridiction consiste à confronter l'acte administratif unilatéral à toute norme hiérarchiquement supérieure. Sont visés par là, les principes généraux du droit, les normes de valeur réglementaire hiérarchiquement supérieures[1513], les normes de valeur législative, la Constitution et les normes supranationales directement applicables.

454.- Les effets du contrôle. À la différence du Conseil d'État qui peut annuler l'acte attaqué, le juge ayant procédé à un contrôle de légalité incident ne peut que refuser d'appliquer l'acte administratif irrégulier[1514]. Celui-ci n'est donc pas supprimé de l'ordonnancement juridique. Il continue d'exister et demeure obligatoire dans les autres litiges, à moins que d'autres juges l'écartent également en vertu de l'article 159 de la Constitution.

Cet effet limité de l'article 159 de la Constitution se marque particulièrement au niveau des transferts de données qui, bien souvent, concernent une masse de citoyens.

> L'exemple qui suit a été soumis pour avis à la CPVP[1515]. Des cas semblables pourraient toutefois être portés devant les cours et tribunaux. L'Inspection bruxelloise du logement recueille des données à caractère personnel relatives à l'immeuble des bruxellois, dans le but de vérifier le respect des exigences de sécurité et de salubrité prescrites par le Code bruxellois du logement. Si elle transfère ces données aux communes, qui s'en servent pour identifier les infractions urbanistiques ainsi que les immeubles qui mériteraient de se voir appliquer un revenu cadastral plus élevé, elle viole notamment l'exigence de compatibilité des finalités des traitements prescrite par la loi du 8 décembre 1992[1516]. Imaginons qu'un tel transfert de données ait lieu, et qu'une commune impose à plusieurs citoyens d'abattre la partie de leur immeuble construite au mépris des règles de l'urbanisme, ou décide de révision le revenu cadastral des immeubles concernés. Un citoyen n'exécute pas les travaux demandés. Il est assigné par la commune qui réclame l'exécution des travaux. Cette personne pourrait invoquer l'illégalité de la décision de la commune, adoptée en violation de la loi du 8 décembre 1992. L'inapplicabilité de la décision de la commune ne vaudra néanmoins que pour ce citoyen et non pour ceux qui se trouvent dans un cas semblable. Elle n'emporte

[1513] Par exemple, un arrêté royal est une norme hiérarchiquement supérieure à un arrêté ministériel.

[1514] Précisons que cela vaut également pour une déclaration de légalité incidente figurant dans un arrêt d'annulation du Conseil d'État.

[1515] CPVP, avis n° 18/2008 du 30 avril 2008 demandé par la Région de Bruxelles-Capitale, Administration de l'Aménagement du Territoire et du Logement, Direction de l'Inspection régionale du Logement relatif à la communication à une administration communale de données recueillies en application du Code bruxellois du Logement.

[1516] CPVP, avis n° 18/2008, *op. cit.*, pp. 4 et s.

pas non plus l'obligation pour la commune ou l'inspection du logement de mettre fin à ces traitements de données illégaux.

L'intérêt d'invoquer l'article 159 de la Constitution devant le juge saisi doit être relativisé dans l'hypothèse où la décision administrative contestée en raison de l'illégalité du traitement de données sur lequel elle se fonde a été prise dans l'exercice d'une compétence liée de l'administration[1517].

Prenons l'exemple d'une loi qui affirme que toute personne dont le revenu est inférieur à 2.000 euros a droit à l'allocation chauffage de la part du CPAS[1518]. Le CPAS exerce une compétence liée, ayant notamment l'obligation de refuser d'octroyer cette allocation aux personnes dont le revenu dépasse 2.000 euros.

Dans cette hypothèse, le juge écarte la décision administrative illégale par application de l'article 159 de la Constitution. Ensuite, pour vider la contestation portée devant lui, il doit appliquer la loi. Cela aboutit à ce que le juge substitue sa décision à celle qu'aurait dû adopter l'administration dans l'exercice de sa compétence liée[1519]. Tantôt, la décision du juge sera semblable à celle de l'administration. Tantôt, elle divergera.

Ainsi donc, il est vain d'invoquer l'exception d'illégalité lorsque l'illégalité du traitement de données réside dans un *transfert de données illégal*, mais que lesdites données sont exactes. En effet, dans ce cas, la décision administrative est écartée par le juge en raison de l'illégalité du transfert de données sur lequel elle se fonde. Mais, ensuite, le juge applique la loi. Il demande aux parties de fournir elles-mêmes les données de manière à pouvoir trancher le litige. La décision du juge ne sera pas différente de la décision de l'administration.

Pour reprendre l'exemple ci-dessus, le CPAS refuse l'octroi de l'allocation chauffage à Gérard Manfroy au motif que le revenu de ce dernier excède 2.000 euros. Cette information est exacte. Elle a néanmoins été communiquée au CPAS sans respecter l'obligation d'obtenir l'autorisation du comité sectoriel compétent imposée par la loi du 8 décembre 1992[1520]. Gérard Man-

[1517] L'administration exerce une compétence liée lorsque la loi lui impose d'adopter un comportement déterminé. À ce sujet, voy. égal. *infra,* n° 457.-

[1518] Cet exemple s'inspire, en le simplifiant, du système d'allocation de chauffage octroyée par le Fonds social Mazout et organisé par les articles 204 et s. de la loi-programme du 22 décembre 2008, *M.B.,* 29 décembre 2009.

[1519] À ce sujet, voy. M. Nihoul et R. Van Melsen, « Les effets de l'art. 159 de la Constitution en matière fiscale sur une contrainte visée dans délégation démontrée », *R.G.C.F.,* 2012/3, pp. 213 à 216.

[1520] Voy. *infra,* n° 534.-

> froy assigne le CPAS en exigeant le paiement de l'allocation de chauffage. Il invoque l'article 159 de la Constitution pour obtenir du juge qu'il écarte la décision de refus fondée sur un transfert de données illégal. Le juge écarte cette décision mais demande qu'on lui fournisse le montant dudit revenu. Compte tenu du fait que ce revenu excède 2.000 euros, le juge refuse l'octroi de l'allocation chauffage.

Par contre, invoquer l'article 159 de la Constitution demeure intéressant lorsque l'illégalité du traitement de données réside dans l'utilisation, par l'administration, de *données erronées*. Dans ce cas, l'administration a violé l'article 4, 4°, de la loi du 8 décembre 1992. Sa décision est écartée. La décision prise par le juge à qui les données exactes ont été communiquées diffère de celle de l'administration.

> C'est erronément que le CPAS considère que le revenu de Gérard Manfroy excède 2.000 euros et refuse de lui octroyer l'allocation chauffage. Le juge écarte cette décision de refus. Se fondant sur des données exactes qui attestent du fait que le revenu de Monsieur Manfroy n'excède pas 2.000 euros, le juge décide qu'il a droit à l'allocation de chauffage.

§2. La contestation directe de certains actes administratifs

455.- Une « bulle de contentieux objectif »[1521]**.** Comme on l'a vu, en principe, la violation du droit objectif et la demande d'annulation de l'acte illégal qui en découle doivent être portées devant le Conseil d'État. Il est toutefois fait exception à ce principe dans certaines matières, ce qui signifie que certaines juridictions judiciaires peuvent annuler des actes administratifs illégaux.

C'est le cas en matière de *sécurité sociale* : le tribunal du travail est compétent, à l'exclusion du Conseil d'État, pour connaître de recours dirigés contre les actes administratifs pris en matière de sécurité sociale, et ce, en vertu des articles 579 à 583 du Code judiciaire. À cet égard, d'aucuns mettent en évidence que « le tribunal du travail dispose de la même capacité de contrôle que le Conseil d'État » et peut ainsi « mettre à néant toute décision liée ou discrétionnaire dans laquelle il aurait décelé des irrégularités que son pouvoir de contrôle [...] lui permettait d'appréhender »[1522].

[1521] Selon l'expression utilisée par Diane Deom (voy. D. Deom, « Le refus d'application », *in L'article 159 de la Constitution. Le contrôle de légalité incident* (dir. M. Nihoul), *op. cit.*, p. 163).

[1522] I. Mathy, « Étendue des pouvoirs du juge à l'égard des décisions prises par une autorité administrative en matière de sécurité sociale », *J.L.M.B.*, 2005, p. 331 et références citées.

Le Conseil d'État ne peut pas non plus connaître de recours formés contre des actes administratifs pris en application d'une *loi d'impôt*. Ces actes administratifs doivent être directement contestés devant le tribunal de première instance, conformément à l'article 569, 32°, du Code judiciaire.

Comme l'affirme Diane Déom, il s'agit là d'une « bulle de contentieux objectif – parce que l'objet même du recours est, par nature, la contestation directe d'un acte administratif, comme devant le Conseil d'État – au sein du contentieux des droits subjectifs – parce que, contrairement au recours pour excès de pouvoir, ce type de contentieux n'implique que le destinataire de l'acte »[1523].

Dans l'e-gouvernement, le contrôle de légalité mené par les juridictions judiciaires compétentes ne suscite pas de réflexions différentes de celles que nous avons développées au sujet du Conseil d'État. Nous y renvoyons donc le lecteur. Toutefois, il convient de souligner qu'il est particulièrement important, pour la juridiction du travail ou le tribunal de première instance, de ne pas négliger la loi du 8 décembre 1992 dans l'examen de légalité des actes administratifs contestés. En effet, jusqu'à présent, c'est en matière de sécurité sociale et en matière fiscale que l'e-gouvernement s'est le plus fortement développé, générant la mise en place d'outils informatiques nouveaux ainsi qu'une multiplication de traitements de données destinés à augmenter l'efficacité de l'administration dans ces matières. Il est donc particulièrement important, dans ces domaines, de veiller au respect des obligations légales qui entourent l'utilisation des données à caractère personnel des citoyens.

> Par exemple, la Banque-Carrefour de la sécurité sociale a été créée au début des années nonante et est le premier outil du genre. Sa mise en place a provoqué une multiplication d'échanges de données entre les institutions de sécurité sociale. C'est aussi pour renforcer l'efficacité des contrôles en matière sociale qu'a été créé le premier entrepôt de données en Belgique, OASIS, qui facilite la prise de décisions en matière de sécurité sociale.
>
> Par ailleurs, les données fiscales intéressent bon nombre d'administrations chargées, par exemple, de calculer une allocation sur la base de la donnée « revenu »[1524]. Les échanges de données entre le SPF Finances et les autres administrations sont donc nombreux. En outre, l'efficacité de la lutte contre la fraude fiscale est régulièrement invoquée pour justifier de nouveaux traitements de données[1525], dont certains sont d'ailleurs critiquables, comme nous l'avons souligné précédemment[1526].

[1523] D. Deom, « Le refus d'application », *op. cit.,* p. 163.
[1524] Voy. *supra,* not. n° 151.- et s.
[1525] Voy. *supra,* not. n° 144.-
[1526] Voy. *supra,* not. n° 133.-

Il en résulte que nombre d'actes administratifs pris en matière de sécurité sociale ou en matière fiscale se fondent aujourd'hui sur des traitements de données. La juridiction du travail et le tribunal de première instance sont donc susceptibles d'examiner de plus en plus souvent la légalité de ces actes administratifs au regard de la loi du 8 décembre 1992.

En particulier, certains aspects de ces traitements de données doivent retenir l'attention de ces juridictions.

Tout d'abord, s'agissant de la sécurité sociale, l'on sait que les institutions de sécurité sociale sont soumises à l'obligation de *collecte indirecte des données*. Rappelons-le, l'article 11 de la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale dispose que « lorsque les données sont disponibles dans le réseau, les institutions de sécurité sociale sont tenues de les demander exclusivement à la Banque-Carrefour ». Il résulte de cette obligation légale qu'une institution de sécurité sociale ne pourrait reprocher à un demandeur d'aide de ne pas avoir fourni des informations que cette institution devait obtenir par elle-même via la Banque-Carrefour de la sécurité sociale.

> C'est ce qu'a reconnu la Cour du travail de Bruxelles dans un arrêt exposé précédemment[1527]. Dans cet arrêt, le juge constate que les CPAS sont soumis à l'article 11 de la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale. Bien que tout demandeur d'un revenu d'intégration sociale est soumis à une obligation de collaboration et doit fournir au CPAS tous les renseignements utiles à sa situation[1528], il n'en demeure pas moins qu'« un manque de collaboration du demandeur ne peut être envisagé à propos d'informations, auxquelles le CPAS peut accéder, accessibles via la Banque-Carrefour de la sécurité sociale »[1529]. Il ne peut donc être reproché au demandeur d'un revenu d'intégration sociale, Monsieur E.G., d'avoir manqué à son obligation de collaboration puisque « la plupart des documents prétendument manquant étaient accessibles via la Banque-Carrefour ou le Registre national : le CPAS n'avait pas à les demander à Monsieur E.G. ; il aurait dû les recueillir d'initiative »[1530]. Monsieur E.G. a donc droit au revenu d'intégration sociale.
>
> La Cour du travail de Liège a raisonné de manière semblable en matière de droit à la pension[1531].

[1527] Voy., *supra,* n° 167.-

[1528] Art. 19, §2, de la loi du 26 mai 2002 concernant le droit à l'intégration sociale.

[1529] C.T. Bruxelles, 21 avril 2010, R.G. n° 2008/AB/51591 et n° 2009/AB/51809, 4e feuillet.

[1530] *Ibid.,* 6e feuillet.

[1531] C.T. Liège, 27 juin 2006, *J.L.M.B.,* 2007, pp. 1043 à 1047. Voy. *supra,* n° 167.-

Ensuite, les données fiscales et les données de sécurité sociale intéressent beaucoup d'administrations qui souhaitent donc les obtenir. Il revient au juge de vérifier *la légalité des transferts de données* pris en amont de la décision administrative contestée, même si ces transferts de données constituent des mesures préparatoires à l'acte administratif. En effet, ainsi qu'on l'a dit lors de notre analyse du Conseil d'État, un acte administratif adopté suite à un transfert de données illégal est fondé sur des motifs illégaux. Son auteur a commis un excès de pouvoir en ne respectant pas les règles de droit qui encadrent les transferts de données. L'acte administratif est illégal et doit être annulé.

> Pour reprendre un exemple expliqué précédemment[1532], si l'Inspection bruxelloise du logement transfère aux communes les données relatives au revenu cadastral des citoyens, l'exigence de compatibilité des finalités des traitements prescrite par la loi du 8 décembre 1992 est violée. Il en va de même de l'exigence de proportionnalité des données, compte tenu du fait que les communes disposent d'autres moyens pour atteindre le même objectif (enquête sur place, consultation des registres de la population, …). La décision de la commune de réviser le revenu cadastral de certains immeubles ou de sanctionner les infractions urbanistiques, serait illégale car elle serait fondée sur des données auxquelles la commune a eu illégalement accès[1533].

Enfin, on ne saurait trop insister sur l'importance d'utiliser des données exactes et à jour. Un acte administratif fondé sur des données erronées peut se voir reprocher la violation de deux législations distinctes. En effet, la motivation d'un tel acte est inadéquate, et viole l'article 3 de la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs.

> C'est ce qu'a décidé le Tribunal du travail de Bruxelles dans une affaire analysée précédemment[1534]. Monsieur S. conteste la légalité d'une décision de l'ONEm lui réclamant le remboursement d'allocations de garantie de revenu. La décision de l'ONEm est fondée sur une donnée à caractère personnel relative aux revenus de Monsieur S. que l'ONEm a reçue de l'INASTI. Malheureusement, cette donnée est erronée. La décision de l'ONEm est annulée, au motif qu'en se fondant sur une donnée inexacte, elle n'est pas motivée adéquatement et viole l'article 3 de la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs[1535].

[1532] Voy. *supra,* n° 454.- Voy. égal. *supra,* n° 49.-

[1533] CPVP, avis n° 18/2008 du 30 avril 2008 demandé par la Région de Bruxelles-Capitale, Administration de l'Aménagement du Territoire et du Logement, Direction de l'Inspection régionale du Logement relatif à la communication à une administration communale de données recueillies en application du Code bruxellois du Logement, pp. 4 et s.

[1534] Voy., *supra,* n° 320.-

[1535] Trib. Trav. Bruxelles, 19 janvier 2009, R.G. n° 69381/98.

Mais on peut également constater que pareille décision administrative viole aussi l'article 4, 3°, de la loi du 8 décembre 1992 qui impose l'utilisation de données exactes et à jour. Partant, l'acte administratif peut également être annulé sur la base de la loi du 8 décembre 1992.

§3. La responsabilité civile de l'administration

456.- L'article 1382 du Code civil. En vertu de l'article 1382 du Code civil, la responsabilité civile de l'administration peut être engagée s'il est établi que cette dernière a commis une faute qui a provoqué un dommage. Toute personne peut donc obtenir réparation du dommage subi suite à la faute commise par l'administration à l'occasion d'un traitement de données à caractère personnel.

La notion de faute est circonscrite avant de porter attention à la réparation du dommage qui s'en suit.

1. La faute

457.- L'établissement de la faute. Les actes de l'administration doivent respecter la loi en raison de sa valeur hiérarchiquement supérieure. C'est pourquoi, les traitements de données effectués dans l'administration doivent respecter la loi du 8 décembre 1992 et les autres législations applicables en la matière.

Dans une jurisprudence déjà largement commentée en doctrine, la Cour de cassation affirme que toute illégalité est une faute[1536]. Cela signifie qu'en ne respectant pas les normes qui lui imposent un comportement déterminé, l'administration se rend coupable d'une faute civile et

[1536] Cass., 19 décembre 1980, *Pas.,* 1981, I, p. 453 ; Cass., 13 mai 1982, *J.T.,* 1982, p. 772 et R.-O. Dalcq, observations sous Cass., 13 mai 1982, *R.C.J.B.,* 1984, pp. 19 à 31 ; Voy. égal. J.-L. Fagnart, « La responsabilité de l'administration du chef d'excès de pouvoir », observations sous Bruxelles, 14 septembre 1979, *A.P.T.,* 1980, pp. 56 à 62 ; du même auteur, « De la légalité à l'égalité », *in La responsabilité des pouvoirs publics,* Bruxelles, Bruylant, 1991, p. 23 ; H. Vandenberghe, « Overheidsaansprakelijkheid. Aansprakelijkheid van de uitvoerende macht », *in Overheidsaansprakelijkheid* (dir. H. Vandenberghe, A. Van Oevelen, H. Vuye, L. Wynant et H. Vandenberghe), Brugge, die Keure, 2005, pp. 7 et s. ; D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.,* p. 183 ; B. Dubuisson, « Faute, illégalité et erreur d'interprétation en droit de la responsabilité civile », note sous Cass. (1e ch.), 26 juin 1998, *R.C.J.B.,* 2001, pp. 28 à 72 ; D. De Roy, « La responsabilité quasi-délictuelle de l'administration : unité ou dualité des notions d'illégalité et de faute ? », *in La protection juridictionnelle du citoyen face à l'administration* (dir. H. Dumont, P. Jadoul et S. van Drooghenbroeck), Bruxelles, La Charte, 2007, pp. 69 à 108 C. Doyen-Biver, A.-L. Durviaux, D. Fisse, J. Sohier, *La responsabilité des pouvoirs publics,* Kluwer, Waterloo, 2010.

ce « sans que l'administration puisse se retrancher derrière le manque de clarté du texte légal ou la diversité des interprétations existant à l'époque où l'acte a été pris »[1537]. Cette jurisprudence prône donc la même solution que celle consacrée par l'article 15*bis* de la loi du 8 décembre 1992 s'agissant du respect des obligations qui s'imposent aux traitements de données à caractère personnel[1538].

> Ainsi, dans son arrêt du 13 mai 1982, la Cour de cassation affirme que « l'autorité administrative commet une faute lorsqu'elle prend ou approuve un règlement qui méconnaît des règles constitutionnelles ou légales lui imposant de s'abstenir ou d'agir de manière déterminée »[1539].

L'administration qui commet une illégalité est exonérée de sa responsabilité si elle peut se prévaloir d'une erreur invincible[1540]. Cette notion fait l'objet d'une appréciation sévère en pratique[1541].

> Par exemple, l'administration peut se prévaloir d'une erreur invincible de droit dans le cas où le législateur adopterait une loi interprétative postérieurement à l'adoption de l'acte administratif fondé sur une interprétation autre de la loi interprétée.

Cette solution est avantageuse pour le citoyen mais sévère pour l'administration, car le concept de « norme imposant un comportement déterminé » est interprété largement par la Cour de cassation[1542]. De plus, cette solution nie le fait qu'en principe, l'existence d'une faute s'apprécie au regard de la situation dans laquelle était placé l'auteur de l'acte au moment où il a commis le fait dommageable. Pour Bernard Dubuisson, l'identité entre la faute et l'illégalité ne respecte pas ce principe, puisque « le contrôle de la légalité d'un acte administratif [...] s'opère objectivement indépendamment de toute appréciation du comportement de l'autorité administrative qui a pris l'acte querellé et du contexte dans lequel cet acte s'inscrivait à l'époque. Sous cet angle,

---

[1537] B. Dubuisson, *op. cit.,* p. 47.

[1538] Voy. *infra,* n° 485.- et s.

[1539] Cass., 13 mai 1982, *Pas.,* 1982, I, p. 1056.

[1540] *Idem.*

[1541] D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.,* p. 183 ; B. Dubuisson, *op. cit.,* p. 47.

[1542] B. Dubuisson, *op. cit.,* pp. 49 à 51 ; X. Thunis, *Théorie générale de la faute,* Vol. 2, Bruxelles, Kluwer, 2006, pp. 9 et 10.

déduire la faute de l'illégalité conduit inévitablement à une objectivation de la faute et donc à une aggravation sensible de la responsabilité de l'administration »[1543].

S'interrogeant également sur cette équation au regard d'un arrêt rendu plus récemment par la Cour de cassation[1544], David De Roy soutient que l'existence d'une faute dans le chef de l'administration doit être appréciée au regard du contenu de la norme applicable à l'espèce. Ainsi, si la norme impose un comportement spécifique à l'administration, cette dernière commet une faute en ne la respectant pas. Si, par contre, la norme ne peut être appliquée sans que l'administration use d'un pouvoir d'appréciation, l'établissement de la faute suppose que l'administration ait manqué au devoir général de prudence que lui impose l'article 1382 du Code civil[1545].

Bien que cette solution soit intéressante, nous ne l'approfondissons pas dans le cadre de cette recherche. À notre sens, même si, pour l'heure, les règles applicables aux traitements de données effectués dans l'e-gouvernement sont difficilement compréhensibles, la combinaison du régime juridique de la protection des données à caractère personnel et des règles du droit administratif impose aux administrations des comportements déterminés. Si ceux-ci ne sont pas respectés, ils sont constitutifs d'une faute au sens de l'article 1382 du Code civil.

> Prenons l'exemple d'une administration qui collecte des données auprès des citoyens. Elle doit notamment veiller au respect de la finalité de ce traitement. Ainsi qu'on l'a vu précédemment, ce concept est encadré assez précisément pour que l'on puisse raisonnablement soutenir qu'il impose un comportement déterminé à l'administration. Celle-ci doit notamment vérifier que la finalité entre dans ses missions légales. La finalité doit également être suffisamment précise, c'est-à-dire que, conformément à la jurisprudence de la CPVP, elle constitue une fin en soi, use de critères fonctionnels, etc.[1546].
>
> Cette administration doit également respecter l'exigence de proportionnalité. Ainsi qu'on l'a vu, cette exigence se dédouble en une exigence de

[1543] B. Dubuisson, *op. cit.,* p. 49. D'autres auteurs émettent des critiques qui s'inscrivent en ce sens. Voy. M. Salmon, note sous Bruxelles, 19 décembre 1972, *J.T.,* 1973, p. 407 ; D. Déom et B. Pâques, « Les permis et autorisations administratives, et la réparation des dommages causés aux tiers », *A.P.T.,* 1995, p. 58.

[1544] Cass., 25 octobre 2005, *J.L.M.B.,* 2005, pp. 638 et s.

[1545] voy. D. De Roy, « La responsabilité quasi-délictuelle de l'administration : unité ou dualité des notions d'illégalité et de faute ? », *op. cit.*, pp. 69 à 108 ; J.-F. Neven et D. De Roy, « Principes de bonne administration et responsabilité de l'O.N.S.S. », *in La sécurité sociale des travailleurs salariés. Assujettissement, cotisations et sanctions* (dir. J.-F. Neven et S. Gilson), Bruxelles, Larcier, 2010, pp. 546 à 552.

[1546] Voy. *supra,* n° 113.- et s.

> proportionnalité du traitement et une exigence de proportionnalité des données. Les critères d'adéquation et de nécessité, consacrés notamment dans la loi du 8 décembre 1992, guident l'administration dans cet examen. Celle-ci est également éclairée par les avis de la CPVP et de la section de législation du Conseil d'État[1547].

De plus, le régime de responsabilité organisé par la loi du 8 décembre 1992 à l'article 15*bis* confirme qu'il faut considérer que la violation des règles qui encadrent les traitements de données s'assimile à une faute de l'administration. Comme nous le développons plus loin[1548], l'article 15*bis* de la loi du 8 décembre 1992 affirme que le responsable de traitement qui viole une obligation prévue par la loi du 8 décembre 1992 est responsable du dommage qui s'en suit. Il découle de cette disposition législative qu'en violant la loi du 8 décembre 1992, l'administration commet une faute, ce qui s'assimile à la solution de la Cour de cassation.

Il n'en demeure pas moins que l'administration est confrontée à un exercice difficile lorsqu'elle doit appliquer les normes relatives à la protection des données à caractère personnel des citoyens. Les développements qui font l'objet des deux premiers titres de la recherche le soulignent à l'envi. Pourtant, c'est un régime de responsabilité sévère qui s'impose à l'administration, comme nous venons de le souligner. Ce constat ne fait que renforcer l'importance et l'urgence de clarifier les règles applicables à l'e-gouvernement[1549].

Ainsi donc, en ne respectant pas les règles de protection des données à caractère personnel, l'administration commet une faute civile. Cette affirmation n'est pas négligeable dans l'e-gouvernement car malgré les progrès de l'informatique, nombre d'erreurs sont encore commises à l'occasion de l'utilisation des données à caractère personnel des citoyens.

> Par exemple, l'administration responsable d'une source authentique de données est chargée d'assurer l'*exactitude des données* qui ont vocation à être communiquées à d'autres administrations. Si elle manque à cette obligation et diffuse une donnée erronée, elle commet une illégalité qui est une faute.
>
> L'administration est également tenue à l'exigence de *proportionnalité des données* qu'elle utilise. Cela implique notamment l'obligation d'utiliser les bonnes données dans le traitement d'un dossier. Or, l'informatique, sous couvert de faciliter la tâche des agents, peut les amener à agir trop

[1547] Voy., *supra,* n° 136.- et s.

[1548] Voy. *infra,* n° 485.- et s.

[1549] À ce sujet, voy. les solutions proposées au premier titre de la recherche, en particulier aux numéros 157.- et s. et au deuxième titre de la recherche, en particulier aux numéros 377.- et s.

rapidement et à utiliser une mauvaise information. En témoigne l'exemple suivant. Un homme a un enfant d'un premier mariage. La caisse d'allocations familiales détient un dossier à son nom, dans lequel est repris le nom de sa première épouse. Après un divorce et un remariage, cet homme a un enfant avec sa deuxième épouse. La deuxième épouse écrit à la caisse d'allocations familiales pour obtenir le versement de l'allocation de naissance du nouveau-né. Souhaitant une précision administrative, la caisse d'allocations familiales écrit… à l'ex-épouse, ayant confondu les adresses de l'épouse et de l'ex-épouse dans le dossier du mari. Une telle erreur provoqua un flot d'injures de l'ex-épouse à l'égard son ex-mari. On n'ose imaginer les erreurs que risquent de subir les citoyens s'étant déjà remariés à plusieurs reprises… Par ailleurs, si la caisse d'allocations familiales n'avait pas eu besoin de précisions supplémentaires, l'allocation de naissance aurait sans doute été versée à l'ex-épouse, ce qui aurait, sans doute, atténué la réaction de cette dernière, mais aurait privé les parents de l'allocation de naissance du nouveau-né.

Dans le même sens, en octobre 2010, l'administration fiscale wallonne envoie une lettre réclamant le paiement de la taxe Télé-redevance à Thierry, un SDF domicilié au CPAS de Namur, son adresse de référence. Comme l'affirme le président du CPAS de Namur, Philippe Defeyt, « avoir une adresse de référence, on sait que ce sont des personnes en difficulté de logement et donc la probabilité qu'elles se promènent avec une télévision est quand même extrêmement faible [...] ce serait quand même bien que l'administration soit attentive aux personnes en difficulté de logement et qu'elle ne leur envoie pas des taxes qui manifestement ne sont pas justifiées dans ce cas ».[1550]

458.- L'imputabilité de la faute. À qui incombe la faute que constitue un traitement illégal de données ?

Le traitement de données étant effectué par une administration, la faute est, en principe, imputable à cette dernière, en vertu de l'article 1382 du Code civil[1551]. Concrètement, qui assigner dans l'hypothèse où une administration prend une décision illégale car fondée sur une donnée inexacte, alors que cette donnée provient d'une source authentique détenue par une autre administration qui aurait dû veiller à l'exactitude de l'information ? Dans ce cas, il semble que le citoyen doive assigner l'administration ayant adopté la décision illégale, à charge pour cette dernière d'appeler en intervention l'institution responsable de la source authentique puisqu'elle a manqué à son obligation d'assurer la fiabilité des données transmises.

[1550] F. Hainaut, « Un SDF doit payer une taxe télé-redevance », www.RTBF.be, 19 octobre 2010.

[1551] D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.,* p. 191.

Peut-on également mettre en cause la responsabilité d'un agent en particulier ?

> Par exemple, les agents de la fonction publique ont accès au Registre national. Des difficultés sentimentales peuvent expliquer la tentation de chercher, par un accès au Registre national, la nouvelle adresse d'une ex petite amie pour guetter les allers et venues de cette dernière[1552]. Il est déjà arrivé également qu'un agent du SPF Finances fasse un usage illégal de Tax-on-web pour modifier sa déclaration fiscale et celle de deux amis[1553].

La réponse est à trouver dans deux lois qui s'appliquent aux personnes travaillant au sein de l'administration, à savoir, la loi du 10 février 2003 « relative à la responsabilité des et pour les membres du personnel au service des personnes publiques »[1554] et la loi du 3 juillet 1978 « relative aux contrats de travail »[1555].

> La loi du 10 février 2003 s'applique aux agents statutaires qui travaillent au sein d'une administration fédérale, régionale, communautaire, provinciale ou communale[1556].
>
> La loi du 3 juillet 1978 s'applique aux agents du service public engagés dans les liens d'un contrat de travail[1557].

Ces deux législations prévoient des règles de responsabilité similaires. Ainsi, lorsqu'un agent commet une faute, dans l'exercice de ses fonctions et en lien avec celles-ci, il doit répondre des agissements qui constituent un dol, une faute lourde ou une faute légère habituelle.

> Dans le cas d'un agent ayant accédé illégalement au Registre national, par exemple, il reviendra au juge du fond d'apprécier la gravité de la faute au regard du but poursuivi par cette consultation, du type de données consultées, de la régularité d'un tel accès illégal, du fait que l'agent avait déjà été mis en garde ou non, etc.

Dans ces hypothèses, l'agent peut être condamné personnellement ou *in solidum* avec la personne publique qui l'engage. Concrètement, la

---

[1552] Pour un cas d'accès illégal au Registre national motivé par des difficultés sentimentales, voy. C.E., *Van Merris,* du 3 avril 2006, n° 157.281.

[1553] À ce sujet, voy. Question n° 0590 de M. Raf Terwingen du 24 août 2008 (F), *Q.R.,* Chambre, 2008-2009, p. 74.

[1554] *M.B.,* 27 février 2003.

[1555] *M.B.,* 22 août 1978.

[1556] D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.,* pp. 191 et 192.

[1557] Les mandataires politiques, en ce compris le ministre, ne semblent visés ni par la loi du 10 février 2003 ni la loi du 3 juillet 1978. À ce sujet, voy. D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.,* pp. 196 à 199.

victime peut assigner en responsabilité la personne publique de qui émane la faute. Celle-ci peut ensuite exercer une action récursoire contre l'agent responsable de la faute[1558]. Il importe dès lorsque l'administration tienne à jour un fichier de *logs* reprenant chaque traitement de données effectué ainsi que l'identité de l'agent responsable et le moment du traitement[1559]. De cette manière, il sera possible d'identifier le responsable de la faute, sans quoi l'administration devrait en répondre seule. À titre préventif, l'administration peut également mettre en place un système qui limite l'accès des agents aux seules données qu'ils ont le droit de connaître dans le cadre de leurs fonctions.

> C'est ce qui se fait, par exemple, au SPF Finances. Un système central, dénommé IAM (*Identity and Access Management*), limite l'accès de chaque agent aux données personnelles des citoyens et ce, en fonction de leur grade, de leur statut, de l'administration à laquelle ils appartiennent etc. De plus, le système IAM tient un journal des accès effectués[1560].

2. Le dommage en lien causal avec la faute et sa réparation

459.- Un dommage et un lien causal. Conformément à l'article 1382 du Code civil, pour obtenir réparation, la victime doit établir un dommage. Elle doit également prouver que, sans l'irrégularité commise par l'administration, le dommage ne serait pas produit tel qu'il s'est produit. À cet égard, la nature de l'illégalité commise est importante, toute illégalité ne présentant pas nécessairement un lien causal avec le dommage dont le citoyen se prévaudrait.

> Par exemple, un citoyen est contraint, par sa commune, d'abattre l'annexe de sa maison, construite au mépris des règles de l'urbanisme. Il découvre que la commune a eu connaissance de l'infraction à partir de données qui lui ont été illégalement transmises par l'inspection du logement. Bien que la commune ait traité illégalement des données, elle aurait eu connaissance de l'infraction en accomplissant, par exemple, une enquête de quartier. Le dommage matériel subi par le citoyen contraint d'abattre l'annexe de sa maison n'est pas lié au transfert illégal de données, mais bien à la loi prescrivant les règles urbanistiques[1561].

[1558] Cette action est prévue par l'article 5 de la loi du 10 février 2003.

[1559] À ce sujet, voy. les développements consacrés à l'*audit trail, supra,* n° 404.- et s.

[1560] À ce sujet, voy. Question n° 0590 de M. Raf Terwingen du 24 août 2008 (F), *op. cit.*, pp. 64 et 65.

[1561] À ce sujet, voy. J.-F. Neven et D. De Roy, *op. cit.,* pp. 554 à 556.

a) Le dommage moral. Un traitement de données illégal peut engendrer un dommage moral, compte tenu du fait que l'administration traite de données relatives à des sphères diverses de la vie du citoyen, dont certaines touchent à des questions très sensibles. L'ampleur de ce dommage variera selon la nature des données illégalement traitées, ou le type de traitement illégal accompli.

> Par exemple, envoyer un rappel de paiement à une personne décédée ne manquera pas de causer un préjudice moral à sa veuve. Il en va de même d'un rappel de paiement d'une taxé télé-redevance envoyée à un SDF.
>
> Des erreurs dans le traitement peuvent également avoir de lourdes conséquences, si l'on pense, par exemple, à une administration fiscale qui publierait involontairement sur internet la liste des contribuables suspectés de fraude fiscale.

Plus largement, compte tenu de l'importance pour l'État de garantir l'autodétermination informationnelle de chaque citoyen, les illégalités commises dans les traitements de données effectués au sein du secteur public peuvent porter gravement atteinte à la confiance du public dans l'administration[1562].

b) Le dommage matériel. Un traitement de données illégal peut également être la cause d'un dommage matériel, telle que la perte d'un droit ou d'une chance. Comme l'affirme la CPVP à propos de la nécessité de garantir l'exactitude des données d'une source authentique, « des données erronées peuvent conduire à ce qu'une personne concernée voie un de ses droits ignoré tandis que l'utilisateur sera confronté de son côté à des contestations de ses décisions qui auraient pu être évitées (frais, travail supplémentaire) »[1563].

> Par exemple, un chômeur se voit refuser les allocations de chômage au motif qu'il n'a pas fourni les documents nécessaires pour prouver son droit. Or, l'ONEm avait l'obligation de se fournir elle-même ces documents en passant par la Banque-Carrefour de la sécurité sociale. L'ONEm a donc manqué à l'obligation de collecte indirecte, qui lui est imposée par la loi du 15 janvier

[1562] À ce sujet, voy. C.E., *Van Merris, op. cit.,* p. 5. Dans ce litige, la Commune d'Uccle impose la sanction disciplinaire de la démission d'office à un fonctionnaire communal ayant illégalement accédé au Registre national. Elle justifie la gravité des faits reprochés en se fondant notamment sur « l'atteinte grave portée à la confiance du public ». Précisons que l'atteinte portée à la confiance du public pourrait entraîner une sanction disciplinaire pour l'agent responsable d'une telle faute, mais ne constitue pas un dommage personnel pour le citoyen.

[1563] CPVP, recommandation n° 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public, n° 31.

1990 relative à la Banque-Carrefour de la sécurité sociale. Le chômeur subit un dommage matériel suite au manquement fautif de l'ONEm.

Autre exemple. Un fonctionnaire se voit refuser une promotion au motif qu'il est atteint d'une maladie, donnée sensible dont l'administration ne pouvait connaître dans le cadre de l'évaluation de l'agent en vue d'une promotion. Cette personne perd la chance d'être promu, en raison d'un traitement illégal de données au sein de l'administration.

460.- La réparation du dommage. La victime d'une irrégularité commise par l'administration peut obtenir la réparation intégrale du dommage subi. Cette réparation peut prendre la forme d'une réparation en nature et/ou d'une réparation par équivalent.

Si l'administration a mal apprécié les conditions légales d'un droit et a, de ce fait, commis une faute, elle peut réparer le dommage en nature, en adoptant un nouvel acte, respectueux des exigences légales.

Si l'ONEm refuse le versement des allocations de chômage au motif qu'il ne dispose pas des documents nécessaires, il peut être condamné à réétudier le dossier du chômeur concerné en trouvant lui-même les renseignements nécessaires par la collecte indirecte de données à laquelle il est astreint.

Si la réparation en nature est insuffisante ou impossible, l'administration peut être condamnée à payer des dommages et intérêts à la victime, ce qui constitue une réparation par équivalent.

L'évaluation pécuniaire du dommage moral subi suite à un traitement de données illégal s'avère délicate. Il y aurait en tout cas lieu de tenir compte de la nature des données traitées et du type de traitement pour évaluer l'ampleur de l'atteinte à la vie privée de la personne concernée.

Section 2. Le contrôle politique

461.- L'article 101 de la Constitution. L'article 101 de la Constitution dispose que « les ministres sont responsables devant la Chambre des représentants ». Pour le dire autrement, la Chambre des représentants exerce un contrôle politique sur l'action du Gouvernement et de l'administration. C'est d'ailleurs sa fonction essentielle aujourd'hui[1564].

Ce contrôle politique s'exerce par trois voies.

[1564] F. Delperee, *Le droit constitutionnel de la Belgique,* Bruxelles, Bruylant, Paris, L.G.D.J., 2000, p. 805.

En posant une *question parlementaire*, un membre de la Chambre des représentants interroge un ministre, par exemple, au sujet du fonctionnement de son administration[1565]. Le ministre est chargé de répondre à la question qui lui a été posée, sans que cela génère un débat ni un vote.

L'*interpellation parlementaire* consiste en une demande adressée par un parlementaire au gouvernement ou à l'un de ses membres. Elle provoque un débat, suivi d'un vote[1566].

Enfin, grâce aux *enquêtes parlementaires*[1567], la Chambre des représentants prend connaissance des d'éléments lui permettant d'apprécier l'action gouvernementale et administrative pour éventuellement la sanctionner.

462.- Le contrôle politique de l'e-gouvernement et la protection des données à caractère personnel. Le régime de la protection des données à caractère personnel offre à la Chambre des représentants des arguments juridiques supplémentaires, pouvant l'aider à affiner son contrôle politique sur le Gouvernement et l'administration. Malheureusement, des embûches expliquent que cet objectif ne soit pas pleinement atteint.

I. Les objectifs du contrôle politique de l'e-gouvernement

463.- L'existence d'une base légale. À l'occasion de son contrôle politique, la Chambre des représentants pourrait examiner la légalité d'un traitement de données à caractère personnel effectué dans une administration et s'étonner que celui-ci ne soit pas fondé sur une base légale.

Comme l'a montré le premier titre de la recherche, l'article 22 de la Constitution et le régime juridique de la protection des données à caractère personnel confèrent un rôle ample au pouvoir législatif. Vu notamment l'importance qu'un débat démocratique soit mené lorsque la vie privée des citoyens est menacée, il revient au législateur de définir les éléments essentiels des outils informatiques mis en place, et des utilisations de données qu'ils génèrent.

Dès lors, si le Gouvernement définit lui-même les éléments cardinaux des traitements de données à caractère personnel effectués dans l'administration, ce qui constitue un débordement de sa compétence d'exécution

[1565] Voy. les art. 122 et s. du Règlement de la Chambre des représentants.

[1566] *Ibid.*, art. 130 et s.

[1567] Art. 56 de la Constitution ; art. 145 et s. du Règlement de la Chambre des représentants.

des lois, la Chambre pourrait user des procédures de contrôle politique pour critiquer lesdits traitements de données illégaux.

464.- Le respect des normes. Le contrôle politique de la Chambre peut également amener cette dernière à vérifier que l'administration effectue les traitements de données à caractère personnels dans le respect des normes qui les encadrent et qui visent à protéger la vie privée des citoyens. À cette occasion, la Chambre peut avoir l'attention attirée par des normes qui fondent un traitement de données mené au sein de l'administration alors qu'elles sont désuètes et devraient donc être modifiées en tenant compte des enjeux de l'informatisation du secteur public.

> Par exemple, une question parlementaire a été posée au Ministre des Finances, à propos de la base légale justifiant l'utilisation, par les agents du SPF Finances, du réseau social *Facebook* pour identifier les contribuables suspectés de fraude, « qui, d'après leur déclaration d'impôt, n'ont que peu de revenus et qui donnent force détails concernant leurs loisirs couteux sur *Facebook*, ou les dirigeants d'entreprise qui déclarent dans leurs frais un voyage d'étude en Chine et qui publient de photos d'excursions en famille […] »[1568]. Une autre question parlementaire à été posée au Ministre des Finances, à propos de la base légale qui fonde les demandes de renseignements qu'adresse l'administration fiscale aux magasins émetteurs d'une carte de fidélité. Ces demandes consistent à réclamer notamment « la liste des contribuables ayant dépensé plus d'une certaine somme pendant une période donnée »[1569]. Dans ces deux cas, le Ministre des Finances a répondu que ces pratiques étaient fondées sur le Code des impôts sur les revenus 1992, en particulier les articles 322 et 323. Or, comme mentionné précédemment dans cette recherche[1570], ces dispositions mériteraient d'être rediscutées en tenant compte des impératifs de la protection des données à caractère personnel.

II. Les embûches du contrôle politique de l'e-gouvernement

465.- Un constat. La protection des données à caractère personnel dans l'e-gouvernement retient-elle suffisamment l'attention de la Chambre des représentants dans l'exercice du contrôle politique ? On est tenté de répondre par la négative. On constate, en effet, que les

[1568] Question n° 0335 de M. Hagen Goyvaerts, du 14 avril 2009 (N), *Q.R.,* Chambre, 2008-2009, 22 juin 2009, p. 95.

[1569] Question n° 0643 de M. Eric van Weddingen, du 4 avril 2001 (F), *Q.R.,* Chambre, 2000-2001, 17 septembre 2001, p. 10470.

[1570] Voy. *supra,* n° 133.-

questions parlementaires relatives à l'informatisation de l'administration sont davantage portées sur le fonctionnement technique et l'efficacité de l'e-gouvernement, que sur le respect de la protection de la vie privée des citoyens.

> Par exemple, lors de la législature précédente (de 2007 à 2010), sur 84 questions parlementaires relatives à la mise en place d'une base de données au sein d'une administration, seules 12 d'entre elles évoquent la question de la protection de la vie privée des personnes concernées. Il est encore plus surprenant de constater que parmi les 72 questions parlementaires qui n'évoquent pas la protection de la vie privée, 5 d'entre elles concernent la mise en place d'un échange de données entre plusieurs administrations dans un but répressif (lutte contre la fraude ou la délinquance). Aucune n'aborde le risque que de tels flux de données portent atteinte à la protection de la vie privée des citoyens concernés.
>
> L'attention des députés est plutôt attirée par des questions techniques, telles que les pannes du système *Tax-on-web* avant l'échéance prévue pour le dépôt des déclarations fiscales[1571]. La lenteur du déploiement de l'e-gouvernement qui nuit à l'efficacité administrative fait également l'objet de questions parlementaires récurrentes. Elles concernent notamment le retard dans la mise en fonctionnement de certaines banques carrefour[1572] ou le fait que des administrations ne bénéficient pas encore de flux de données qui leur sont nécessaires pour automatiser certaines procédures[1573].

Plusieurs facteurs peuvent expliquer un tel constat, comme l'exposent les lignes qui suivent.

466.- La difficulté de comprendre la matière. On l'a déjà dit, le régime juridique de la protection de la vie privée et des données à caractère personnel est parsemé de concepts techniques et de règles floues qui le rendent complexe. On peut raisonnablement penser que, comme maints juristes et citoyens, les députés sont découragés d'approfondir cette matière voire même d'en prendre connaissance.

[1571] Voy. not., la question n° 347 de M. Kattrin Jadin du 28 avril 2011 (F), *Q.R.,* Chambre, session 2010-2011, 6 juin 2011, pp. 6 et 7.

[1572] Voy. not. deux questions qui concernent le fonctionnement de la Banque-Carrefour des véhicules : Question n° 230 de M. Karin Timmerman du 27 septembre 2011 (N.), *Q.R.,* Chambre, 2011-2012, 24 novembre 2011, pp. 95 et s. ; Question n° 019 de M. Georges Gilkinet du 23 janvier 2012 (F.), *Q.R.,* Chambre, 2011-2012, 6 février 2012, p. 364.

[1573] Question n° 031 de M. Maggie De Block du 9 mai 2011 (N.), Chambre, 2010-2011, 18 juillet 2011, pp. 323 et s. (à propos de l'échange de certaines données relatives aux personnes handicapées bénéficiaire d'une allocation d'intégration) ; Question n° 135 de M. Franco Seminara du 14 janvier 2011 (F.), Chambre, 2010-2011, 27 avril 2011, pp. 111 et s. (à propos du croisement de données pour lutter contre la fraude en matière sociale).

La difficulté de comprendre la matière se manifeste au travers des questions parlementaires et parfois même, des réponses des ministres interrogés.

> Par exemple, se souciant de la mise en place de la collecte unique des données au sein de l'Administration flamande, une parlementaire a demandé au Ministre de l'Intérieur si le Registre national allait « délivrer le mandat » permettant à l'Administration flamande de l'Agriculture et de la Pêche d'accéder aux données du Registre national. Le Ministre de l'Intérieur lui a répondu, à juste titre, que la demande d'accès ne devait pas être introduite auprès du Registre national, mais bien auprès du Comité sectoriel du Registre national institué au sein de la CPVP. Il a ajouté, de manière erronée, que cette institution relevait de la compétence du Ministre de la Justice à qui il a transmis ladite question parlementaire[1574]. Le Ministre de la Justice, saisi de la même question, a répondu que le Registre national relevait de la compétence du Ministre de l'Intérieur et a renvoyé la question à celui-ci[1575].

Par ailleurs, compte tenu de l'existence de la CPVP, certains députés sont probablement enclins à faire confiance à cette institution pour veiller au respect des règles de protection des données à caractère personnel et à ne pas examiner eux-mêmes cette problématique. Néanmoins, des parlementaires s'interrogent tout de même sur la légalité de certains traitements et s'étonnent de la passivité de la CPVP. Malheureusement, aucun ministre ne peut apporter de réponses à ces questions parlementaires compte tenu du fait que, depuis une réforme législative intervenue en 2003, la CPVP est rattachée à la Chambre des représentants et n'est plus soumise au contrôle de tutelle du Ministre de la Justice[1576].

467.- La difficulté d'identifier les illégalités. Les membres de la Chambre des représentants peuvent éprouver des difficultés à percevoir les illégalités commises dans le développement de l'e-gouvernement. En effet, on imagine difficilement qu'un ministre veille à assurer la publicité d'un nouvel outil informatique peu respectueux de la vie privée des citoyens. On constate ainsi que nombre de questions parlementaires en ce domaine font suite à une révélation dans la presse ou des plaintes de citoyens. Néanmoins, de telles divulgations demeurent encore trop rares.

[1574] Question n° 454 de M. Maggie De Block, du 9 juin 2011, *Q.R.,* Chambre, 2010-2011, 29 septembre 2011, p. 177.

[1575] Question n° 601 de M. Maggie De Block, du 19 septembre 2011, *Q.R.,* Chambre, 2011-2012, 4 novembre 2011, p. 82.

[1576] Voy. *infra,* n° 487.-

Entre autres exemples, la question parlementaire relative à l'utilisation, par les agents du SPF Finances, de *Facebook* pour identifier des fraudeurs présumés, fait suite à un article publié dans le quotidien *Het Nieuwsblad* le 13 décembre 2008.

*

Conclusions

Ce premier chapitre a montré combien le droit fondamental à la protection de la vie privée et le régime de la protection des données à caractère personnel renforcent les contrôles organisés par le droit administratif.

À présent, les contrôles juridique et politique de l'administration sont affinés grâce à des règles nouvelles qui permettent aux différentes institutions en charge de ces contrôles de s'immiscer dans les « coulisses » de l'administration.

Par exemple, un échange de données entre administrations constituait, hier, une simple mesure préparatoire d'un acte administratif. Il ne pouvait être contesté comme tel. Aujourd'hui, ce même échange doit respecter les exigences légales de la protection des données, à défaut de quoi, il constitue un motif illégal susceptible d'entraîner l'annulation, par le Conseil d'État, de la décision administrative à laquelle il a abouti.

De nombreux autres exemples ont souligné la pertinence des arguments que les règles de protection des données apportent à la Cour constitutionnelle, aux cours et tribunaux, à la Chambre des représentants dans le cadre de son contrôle politique, au Médiateur et à la CADA.

Si les règles de protection des données à caractère personnel renforcent les contrôles traditionnels, l'inverse est vrai également. Les contrôles traditionnels assurent une meilleure protection des données. En effet, ces contrôles traditionnels permettent un examen *ex ante,* au moment où les traitements de données envisagés sont encore à l'état de projet. À cet égard, on a souligné la richesse des avis de la section de législation du Conseil d'État. D'autres contrôles interviennent *ex post,* et concernent les traitements de données déjà accomplis qui suscitent des contestations. Le Médiateur et la CADA sont aisément saisis. Leur intervention peut s'avérer utile, bien qu'elle n'aboutisse pas à une solution contraignante pour l'administration. Par ailleurs, le travail accompli par la Cour constitutionnelle, le Conseil d'État et les cours et tribunaux renforce concrètement la protection des données à caractère personnel dans l'administration, compte tenu des sanctions importantes qu'ils sont en mesure d'imposer

à l'égard des normes et des agissements illégaux. En outre, le contrôle politique qu'exerce la Chambre des représentants sur l'action du Gouvernement doit inciter les ministres à porter attention aux traitements de données effectués dans les administrations qui agissent sous leur contrôle, au risque de voir leur responsabilité politique engagée.

Il n'en demeure pas moins que les contrôles traditionnels révèlent des faiblesses dans le contexte de l'e-gouvernement. Ils ne permettent pas de contester un traitement de données en lui-même, indépendamment de l'acte administratif à laquelle il aboutit[1577]. Ainsi, un citoyen ne peut contester un transfert de données illégal entre deux administrations. Il ne peut qu'attendre qu'une décision administrative soit prise sur la base des données échangées, et contester ensuite la décision. De plus, on remarque que les citoyens usent peu de ces voies d'action pour contrôler l'e-gouvernement.

Ces constats confirment tout l'intérêt des contrôles organisés par le régime de la protection des données à caractère personnel que nous analysons dans le chapitre qui suit.

*

[1577] Sans doute cette assertion doit-elle être nuancée s'agissant du Médiateur fédéral, du moins s'il s'estime compétent pour connaître de ce problème et ne le renvoie pas à la CPVP.

CHAPITRE II.

L'e-gouvernement et le contrôle organisé par le régime juridique de la protection des données à caractère personnel

468.- Des voies de contrôle originales. Le régime de la protection des données à caractère personnel prévoit des voies de contrôle qui complètent utilement les mécanismes issus du droit administratif.

Tout citoyen dispose de moyens d'action particuliers qu'il peut exercer directement à l'égard des administrations détenant des données à son sujet. De plus, deux actions judiciaires particulières sont organisées, plus adaptées aux traitements de données à caractère personnel que l'action en responsabilité fondée sur l'article 1382 du Code civil.

En outre, une autorité de régulation dans le secteur des traitements de données à caractère personnel est instituée. Il s'agit de la Commission de la protection de la vie privée (ci-après, « CPVP »), dont le statut et les moyens d'action retiennent l'attention.

Enfin, les règles de protection des données organisent la possibilité d'instituer des détachés à la protection de la vie privée dans les administrations. Cette nouvelle fonction professionnelle devra être créée prochainement en Belgique, dès l'entrée en vigueur du règlement européen sur la protection des données à caractère personnel.

*

Section 1. Le contrôle à l'initiative de la personne concernée

469.- Une prise concrète sur les données à caractère personnel. La loi du 8 décembre 1992 concrétise le droit à l'autodétermination informationnelle en garantissant à tout citoyen une maîtrise de ses données personnelles. Cette garantie s'exerce par plusieurs voies d'action.

Toute personne peut ainsi saisir l'administration responsable du traitement de ses données en invoquant ses droits de rectification, d'opposition

ou d'interdiction. Elle peut également porter plainte à la CPVP. Deux recours judiciaires sont par ailleurs organisés. L'un, consacré à l'article 14 de la loi du 8 décembre 1992, consiste en la saisine du président du tribunal de première instance statuant comme en référé. L'autre est une action en réparation et est organisé à l'article 15*bis* de la loi du 8 décembre 1992.

I. Les droits de rectification, d'opposition et d'interdiction

470.- L'exercice des droits de rectification, d'opposition et d'interdiction. Si, en accédant à ses données à caractère personnel[1578], un citoyen constate une erreur affectant ses données ou une utilisation illégale de ses données, il peut demander la rectification des données erronées, s'opposer à leur traitement ou réclamer l'interdiction de les conserver ou de les utiliser[1579].

Dans le chapitre précédent, nous avons regretté l'impossibilité de contester ou de corriger un traitement de données en cours, par les voies de contrôle traditionnel. Remarquons qu'en l'occurrence, grâce au régime de la protection des données à caractère personnel, la personne concernée peut effectuer un contrôle préventif, afin d'obtenir la correction des erreurs éventuelles avant que la décision administrative soit prise.

> Le droit de *rectification* est consacré à l'article 12, §1, alinéa 1, de la loi du 8 décembre 1992 qui prévoit que « toute personne a le droit d'obtenir sans frais la rectification de toute donnée à caractère personnel inexacte qui la concerne ».
>
> Le droit d'*opposition* est consacré à l'article 12, §1, alinéa 2, de la loi du 8 décembre 1992 en vertu duquel « toute personne a en outre le droit de s'opposer, pour des raisons sérieuses et légitimes tenant à une situation particulière, à ce que des données la concernant fassent l'objet d'un traitement ». Néanmoins, cette disposition prévoit une exception d'importance pour les traitements de données effectués par les administrations puisque le droit d'opposition ne peut être exercé lorsque « la licéité du traitement est basée sur les motifs visés à l'article 5, b) et c) [de la loi du 8 décembre 1992] ».
>
> Le droit de d'*interdiction*[1580] est consacré à l'article 12, §1er, alinéa 5, de la loi du 8 décembre 1992 qui prévoit que « toute personne a également le

[1578] Convention n° 108, art. 8, b) ; Directive 95/46, art. 12, a) ; Loi du 8 décembre 1992, art. 10.

[1579] Convention n° 108, art. 8, c) ; Directive 95/46, art. 12, b) ; Loi du 8 décembre 1992, art. 12.

[1580] Par souci de clarté, nous parlons de « droit d'interdiction » pour viser la prérogative consacrée à l'art. 12, §1er, al. 5, de la loi du 8 décembre 1992 qui concerne la suppression des données – c'est-à-dire, l'interdiction de les conserver – et l'interdiction de les traiter.

> droit d'obtenir sans frais la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui, compte tenu du but du traitement, est incomplète ou non pertinente ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée ».

La personne qui souhaite exercer ces droits doit adresser une demande au responsable du traitement ou à toute autre personne désignée par le Roi. Ces droits étant personnels, la personne concernée doit prouver son identité en joignant une photocopie de sa carte d'identité, comme le rappelle la CPVP sur son site internet[1581]. La demande doit être datée et signée[1582]. Elle peut être envoyée par la poste, par fax, par un courriel revêtu d'une signature électronique ou déposée sur place.

A. L'utilité des droits de rectification, d'opposition et d'interdiction

471.- Un corollaire du droit d'accès. Les droits de rectification, d'opposition et d'interdiction sont des corollaires du droit d'accès consacré à l'article 10 de la loi du 8 décembre 1992[1583].

472.- Comparaison avec la loi sur la publicité de l'administration. Un droit de rectification est également consacré par la loi du 11 avril 1994 sur la publicité de l'administration. Néanmoins, il souffre des mêmes embûches que celles qui affectent l'accès aux documents administratifs organisé par cette loi du 11 avril 1994[1584].

> L'article 7 de la loi du 11 avril 1994 consacre également un droit de rectification en prévoyant que « lorsqu'une personne démontre qu'un document administratif d'une autorité administrative fédérale comporte des informations inexactes ou incomplètes la concernant, cette autorité est tenue d'apporter les corrections requises sans frais pour l'intéressé. La rectification s'opère à la demande écrite de l'intéressé, sans préjudice de l'application d'une procédure prescrite par ou en vertu de la loi ».

Les droits de rectification, d'opposition et d'interdiction consacrés par la loi du 8 décembre 1992 s'avèrent plus riches dans leur contenu, plus

---

[1581] http://www.privacycommission.be/fr/exercice-droit-opposition/regles

[1582] La CPVP met à disposition des citoyens une lettre type pour l'exercice du droit d'opposition http://www.privacycommission.be/fr/exercice-droit-opposition/regles

[1583] Voy. *supra,* n° 330.- et s.

[1584] Voy. *supra,* n° 252.- et s.

aisés dans leur exercice, et mieux sanctionnés que ce qu'offre le droit administratif traditionnel.

473.- Des droits plus riches. L'article 7 de la loi du 11 avril 1994 ne consacre qu'un droit de rectification. Par contre, en exerçant les droits consacrés à l'article 12 de la loi du 8 décembre 1992, la personne concernée peut non seulement exiger la rectification des données inexactes, mais également s'opposer à leur utilisation[1585]. Par ailleurs, le droit d'interdiction donne un pouvoir très large au citoyen qui peut être amené à intervenir lui-même dans l'évaluation des moyens utilisés par l'administration pour accomplir ses missions. En effet, l'exercice du droit d'interdiction suppose que la personne concernée évalue elle-même la pertinence des données utilisées par l'administration au regard du but poursuivi par cette dernière.

Comme l'a montré le premier titre de la présente recherche, les données utilisées par l'administration devraient idéalement être définies par ou en vertu de la loi. Néanmoins, pour l'heure, il ne s'agit bien souvent que d'un vœu pieu, ce qui rend d'autant plus important le contrôle, par le citoyen, de la légalité des traitements de données effectués par l'administration.

L'article 12 de la loi du 8 décembre 1992 donne également une large prérogative au citoyen en ce qu'il peut contester les traitements de données « interdits », ce dernier terme visant de nombreuses hypothèses.

> Sont ainsi visés les transferts de données qui contreviennent à une obligation imposée par la loi du 8 décembre 1992. Il peut s'agir de traitements poursuivant une finalité indéterminée. C'est le cas, par exemple, lorsque la finalité du traitement n'a pas été déclarée auprès de la CPVP ou si le responsable du traitement n'en a pas informé les personnes concernées.
>
> Sont également interdits, les traitements de données qui poursuivent une finalité incompatible avec le but poursuivi lors de la collecte initiale des informations. Ainsi, une administration qui collecterait indirectement des données pour accomplir une finalité incompatible avec la finalité de la source authentique accomplirait un traitement de données interdit.
>
> Un citoyen pourrait également utiliser ce recours pour contester le fait qu'une administration effectue des traitements de données qui dépassent le cadre des missions qui lui ont été légalement dévolues. Ce peut être le cas lorsque le traitement de données poursuit une finalité n'entrant pas dans les missions légales de l'administration ou lorsque les données utilisées sont disproportionnées.

[1585] Sous réserve toutefois d'une importante exception analysée ci-après.

> On pourrait ainsi remettre en cause les traitements de données effectués par les administrations lorsqu'ils ne reposent sur aucune base légale[1586].

Enfin, les données erronées ou interdites d'utilisation peuvent avoir été communiquées à des destinataires. L'article 12, §3, de la loi du 8 décembre 1992 impose à l'administration responsable d'informer ces destinataires des corrections ou effacement de données. La loi du 11 avril 1994 ne prévoit pas pareille obligation ce qui pourrait contribuer à la propagation d'informations erronées au sein de l'administration.

474.- Des droits plus aisés. Même si l'exercice des droits consacrés à l'article 12 de la loi du 8 décembre 1992 n'est pas sans entrave, il est plus aisé d'obtenir la rectification des données à caractère personnel par l'application de la loi du 8 décembre 1992 plutôt que la loi du 11 avril 1994, pour les raisons exposées précédemment[1587].

En effet, un administré peut, certes, obtenir la correction de ses informations personnelles en vertu de la loi du 11 avril 1994. Mais, rappelons-le, d'une part, il ne peut avoir connaissance de ces erreurs qu'à l'occasion de la consultation d'un document administratif. En d'autres termes, pour vérifier l'exactitude des données utilisées par l'administration, il doit identifier le document administratif susceptible de contenir les données erronées – ce qui n'est pas toujours chose aisée – et ensuite en réclamer l'accès. Par contre, en vertu de la loi du 8 décembre 1992, la personne intéressée peut accéder à ses données sans identifier précisément un document qui les contiendrait. Elle peut se contenter de demander à l'administration la communication de toutes les informations détenues à son sujet.

D'autre part, l'accès aux documents administratifs en vertu de la loi du 11 avril 1994 est assorti d'exceptions plus nombreuses que l'accès aux données à caractère personnel en vertu de la loi du 8 décembre 1992.

475.- Des droits mieux sanctionnés. Si l'administration ne réagit pas à la demande du citoyen ou rejette la demande de rectification, la loi du 11 avril 1994 exige que cette personne adresse une demande de reconsidération à l'administration concernée. Elle peut ensuite intenter un recours au Conseil d'État. Le Conseil d'État pourra au mieux annuler la décision de rejet de l'administration mais non condamner cette dernière à exécuter les rectifications requises.

[1586] On pense, notamment, aux communications de données vers l'entrepôt de données OASIS et la collecte des données issues de OASIS.

[1587] Voy. *supra,* Titre II.

Par contre, en vertu de la loi du 8 décembre 1992, la personne concernée dispose de moyens d'action organisés spécifiquement par cette loi. Ainsi, elle peut porter plainte à la CPVP, qui engage éventuellement une procédure de médiation avec l'administration concernées[1588]. Elle peut également saisir le président du tribunal de première instance dans le cadre de la procédure organisée par l'article 14 de la loi du 8 décembre 1992[1589].

B. La difficulté d'exercer les droits de rectification, d'opposition et d'interdiction dans l'e-gouvernement

476.- Droit d'opposition. Il n'est pas exagéré d'affirmer que le droit d'opposition est une illusion dans l'e-gouvernement. En effet, ce droit ne peut être exercé à l'égard des traitements « nécessaires au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance »[1590]. Or, ce cas de figure couvre les traitements de données effectués par une administration étant donné que les compétences de cette dernière lui sont attribuées par le législateur[1591].

477.- Droits de rectification et d'interdiction. Le manque d'effectivité des droits de rectification et d'interdiction tient tant à l'administration qu'à la personne concernée.

a) Le manque d'effectivité dû à l'administration. Comme on l'a dit, l'administration qui a effectué des corrections aux données ou a procédé à des effacements de celles-ci doit en avertir les destinataires, en vertu de l'article 12, §3, de la loi du 8 décembre 1992.

Cette obligation suppose que l'administration ait connaissance des destinataires de ces données. Or, on peut raisonnablement penser que, bien souvent, ce n'est pas le cas. En effet, la loi ne prévoit pas expressément l'obligation de conserver les destinataires des données transmises. Ce constat conforte d'autant plus la nécessité d'instaurer un cadastre des interconnexions de données[1592].

[1588] La CPVP met à disposition des citoyens une lettre type pour demander une médiation http://www.privacycommission.be/fr/exercice-droit-opposition/regles

[1589] Voy. *infra,* n° 480.- et s.

[1590] Art. 5, c) de la loi du 8 décembre 1992 auquel se réfère l'art. 12, §1er, al. 2, de la loi du 8 décembre 1992.

[1591] Voy. *supra,* Titre I.

[1592] Voy. *supra,* n° 392.- et s.

Remarquons qu'avant la modification, en 1998, de la loi du 8 décembre 1992 suite à la transposition de la directive 95/46, cette loi disposait que, pour permettre la communication des rectifications, le Roi pouvait prévoir un délai durant lequel le responsable du traitement pouvait conserver l'identité des personnes à qui il avait communiqué des données. Ce délai avait été fixé à douze mois. Cette possibilité a néanmoins été supprimée par la modification législative de 1998.

Par ailleurs, le responsable du traitement peut être libéré de l'obligation de communiquer les rectifications aux destinataires des données si pareille notification paraît impossible ou implique des efforts disproportionnés. La CPVP le désapprouve.

> Elle affirme ainsi que « la pondération proposée ici ne se déroule que dans le chef du responsable du traitement, tandis qu'on s'attendrait plutôt à ce que la pondération, qui est effectivement souhaitable, concerne le dommage causé à la personne concernée. Lorsque le dommage dû à des communications fautives matérielles ou psychiques est important pour la personne concernée, on peut s'attendre à ce que le responsable se donne « beaucoup de mal ». C'est pourquoi le texte néerlandais de la directive européenne utilise, à juste titre, le mot « *onevenredig* » au lieu de « *onredelijk* » à l'article 12, §3, premier alinéa, in fine en projet »[1593].

b) Le manque d'effectivité dû à la personne concernée. L'exercice des droits de rectification et d'interdiction suppose que la personne ait connaissance des traitements de données qui la concernent. En outre, une dose certaine de courage est nécessaire pour identifier l'administration responsable du traitement, lui écrire et, le cas échéant, engager une procédure de médiation auprès de la CPVP. Face à de pareilles difficultés, on peut raisonnablement penser que les droits de rectification et d'interdiction dans l'administration sont un leurre.

En ce sens, François Rigaux affirme que « ce n'est pas le moindre des paradoxes – car le droit de la protection de la vie privée en abonde – que pour mieux garantir cette liberté, il faille instaurer un système tellement compliqué et sophistiqué que le citoyen moyen est hors d'état de défendre lui-même son droit à la confidentialité et au secret »[1594]. L'autorité de

[1593] CPVP, avis n° 30/96 du 13 novembre 1996 relatif à un avant-projet de loi adaptant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel à la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, n° 37.

[1594] F. Rigaux, « Chapitre 3. Les paradoxes de la protection de la vie privée » in *Rapport n° 1 sur Internet et la vie privée,* p. 39, disponible à l'adresse http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport1/chapitr3.pdf

contrôle en matière de protection des données est ainsi « chargée de la tutelle des personnes dont la vie privée est menacée. Tutelle est ici une expression rigoureusement exacte, l'expérience ayant démontré que les particuliers n'usent guère des voies d'accès et de recours que le législateur leur a ouvertes à titre individuel »[1595].

Le même constat est dressé en France où « dans la pratique, les droits des usagers sont restés assez formels, celui-ci n'ayant qu'une faible connaissance des fichiers détenant des données sur lui. Le contrôle des traitements est surtout l'affaire de la CNIL ».[1596]

II. Le dépôt de plainte

478.- L'article 31 de la loi du 8 décembre 1992 et le règlement d'ordre intérieur. Toute personne qui estime que ses données ont été traitées illégalement, notamment par l'administration, peut porter plainte auprès de la CPVP, conformément à l'article 31 de la loi du 8 décembre 1992.

> La loi du 8 décembre 1992 met en œuvre une possibilité prévue par l'article 1.2 b) du Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel selon lequel « chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel relevant de sa compétence ».
>
> Une même possibilité est prévue à l'article 28, §4, de la directive 95/46 qui dispose que « chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée de suites données à sa demande ».

La procédure de dépôt de plainte est organisée par l'article 31 de la loi du 8 décembre 1992 et par les articles 25 à 36 du règlement d'ordre intérieur de la CPVP[1597].

Toute personne qui justifie d'un intérêt peut déposer plainte auprès de la CPVP, en envoyant à cette dernière un courrier daté et signé[1598]. Si

---

[1595] *Idem.*

[1596] H. Maisl, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », *in L'administration électronique au service des citoyens »* (dir. G. Chatillon et B. du Marais), Bruxelles, Bruylant, 2003, p. 352.

[1597] Ce règlement d'odre intérieur est disponible à l'adresse http://www.privacycommission.be/sites/privacycommission/files/documents/reglement_ordre_interieur_cpvp.pdf

[1598] Art. 31 de la loi du 8 décembre 1992.

la plainte est envoyée par courriel, elle doit être revêtue d'une signature électronique[1599]. S'en suit alors une procédure qui, en principe[1600], maintient secrète l'identité du plaignant. En outre, les droits de la défense et le principe du contradictoire doivent être respectés. C'est pourquoi, en vertu du règlement d'ordre intérieur de la CPVP, le responsable du traitement a le droit de fournir des informations et des explications nécessaires à la bonne compréhension de l'affaire[1601].

Si la plainte est recevable, la CPVP tente de concilier les parties dans le cadre d'une procédure de médiation. Elle peut, à cette occasion, inviter le responsable du traitement à respecter, le cas échéant, les droits du plaignant, tels que le droit d'accès et le droit d'opposition analysés au chapitre précédent.

Si la médiation aboutit à la conciliation des parties, la CPVP dresse un procès-verbal de l'accord. Si la médiation échoue, la CPVP émet un avis sur le caractère fondé de la plainte, et peut accompagner cet avis de recommandations adressées au responsable du traitement. L'avis de la CPVP accompagné des éventuelles recommandations sont communiqués aux parties concernées, et une copie est envoyée au Ministre de la Justice.

479.- La qualification de « plainte ». Le courrier par lequel une personne dénonce des faits auprès de la CPVP doit mentionner clairement qu'il constitue une plainte. En effet, si « la lecture [du courrier] ne permet pas de conclure avec certitude qu'il s'agit à proprement parler d'une plainte »[1602], le règlement d'ordre intérieur permet à la CPVP d'examiner « s'il est possible de donner une réponse satisfaisante et efficace au problème posé sans devoir suivre la procédure prévue pour le traitement des plaintes »[1603]. Cela signifie que si une personne adresse un courrier à la CPVP dans lequel elle dénonce les agissements d'un responsable de traitement en particulier, sans toutefois mentionner qu'elle porte plainte[1604],

[1599] Art. 25, §1, du règlement d'ordre intérieur de la CPVP.

[1600] En vertu de l'article 26 du règlement d'ordre intérieur, l'identité du plaignant est maitenue secrète sauf si l'examen de la plainte requiert sa divulgation et que le plaignant y a consenti.

[1601] Art. 30 du Règlement d'ordre intérieur de la CPVP disponible à l'adresse http://www.privacycommission.be/sites/privacycommission/files/documents/reglement_ordre_interieur_cpvp.pdf

[1602] Art. 25, §3, du règlement d'ordre intérieur de la CPVP.

[1603] *Idem*.

[1604] Une personne pourrait rédiger un courrier dans lequel la personne demande l'avis de la CPVP au sujet des pratiques d'un responsable du traitement. Cette demande risque d'être considérée comme un courrier qui « ne permet pas de conclure avec certitude qu'il s'agit à proprement parler d'une plainte ». Dès lors, la CPVP pourra y répondre sans entendre le responsable de traitement visé dans le courrier.

la CPVP pourra répondre à ce courrier sans entendre le responsable de traitement concerné.

Cette méthode est critiquable. D'une part, la loi du 8 décembre 1992 n'attribue nullement à la CPVP le pouvoir de se prononcer en dehors des avis, des recommandations et des réponses à une plainte. Le fait, pour la CPVP, de répondre à un courrier qui vise un responsable de traitement en particulier sans respecter les droits de la défense comme elle doit le faire pour les recommandations et les réponses aux plaintes, est donc illégal. D'autre part, le président de la CPVP se prononce sur la légalité d'une pratique menée par un responsable de traitement en particulier – que ce soit dans le cadre d'une recommandation adressée à celui-ci, ou dans une réponse apportée à un citoyen qui interroge la CPVP au sujet de cette pratique. Dans ce cas, il est important que le responsable de traitement visé puisse donner son point de vue avant que la CPVP se prononce. En effet, les recommandations de la CPVP sont accessibles au public, notamment à partir du site internet de la CPVP. Elles sont également communiquées au Ministre de la Justice. Quant aux réponses que le président de la CPVP fournit aux citoyens, elles ne sont pas confidentielles, si bien qu'elles pourraient être rendues publiques par la voie de la presse notamment. Dès lors, si les analyses juridiques du président de la CPVP sont fondées sur des faits erronés, elles risquent de porter injustement atteinte à la réputation du responsable du traitement concerné.

> Ce problème est d'ailleurs apparu dans une affaire opposant Anne-Marie Lizin à la CPVP. À l'origine de cette affaire, un conseiller communal reprochait à Anne-Marie Lizin d'effectuer des traitements de données illégaux, notamment en utilisant les données du CHR de Huy pour envoyer une carte de prompt rétablissement aux personnes qui venaient de sortir de l'hôpital[1605]. Ce conseiller communal a écrit à la CPVP pour connaître son point de vue sur ces agissements, sans porter plainte. La CPVP a répondu que « l'usage ainsi fait des coordonnées des patients constituait un traitement ultérieur de données incompatible avec les finalités du traitement primaire et donc contraire au prescrit de l'article 4 de la loi vie privée ». Puisque le conseiller communal n'avait pas porté plainte, Anne-Marie Lizin n'a pas été entendue par la CPVP et n'a pu donner son point de vue sur les faits. Ledit conseiller communal a ensuite fait part de l'analyse de la CPVP dans la presse, qui a relayé cette analyse. Anne-Marie Lizin, se sentant victime d'une atteinte à sa réputation sans avoir été entendue par la CPVP, a attaqué la réponse de la CPVP devant le Conseil d'État. Finalement, la CPVP a retiré l'acte attaqué et le Conseil d'État a constaté qu'il n'y avait plus lieu de statuer et a condamné la CPVP aux dépens[1606].

[1605] Sur cette affaire, voy. *infra* n° 518.-

[1606] C.E., arrêt *Lizin,* n° 211.698 du 2 mars 2011.

Le responsable de traitement et la CPVP elle-même ont avantage à ce que les droits de la défense soient respectés lorsqu'une personne adresse un courrier à la CPVP pour critiquer les agissements d'un responsable de traitement clairement identifié.

En effet, avant que la CPVP se prononce, le *responsable de traitement* doit pouvoir contester la réalité des faits reprochés, le cas échéant, sous peine d'être injustement critiqué. De cette manière, la CPVP pourra analyser le problème de la manière la plus objective possible. De plus, on ne peut pas ignorer que les règles de protection des données sont complexes. Le responsable d'un traitement de données a peut-être cru, de bonne foi, qu'il agissait conformément à ce régime juridique. Dès lors, en instaurant un dialogue avec le responsable de traitement, la CPVP peut mettre en évidence les aspects problématiques des traitements de données réalisés. Elle pourrait ainsi inciter le responsable du traitement à se conformer aux règles applicables de manière à ne pas devoir adopter de recommandation le concernant ou adapter en conséquence les courriers adressées aux citoyens. Cela répond d'ailleurs pleinement à la mission de la CPVP de fournir des informations sur les règles de protection de la vie privée en général[1607].

Par ailleurs, la *CPVP* est légalement obligée de respecter les droits de la défense quand elle s'adresse à un responsable de traitement en particulier. Le respect de cette obligation diminue donc les risques que le responsable de traitement intente un recours judiciaire à son encontre.

> Ainsi qu'on l'a dit précédemment, l'article 30, §2, affirme qu' « avant d'adresser une recommandation au responsable du traitement, la Commission lui donne l'occasion de faire valoir son point de vue ». Quant à l'article 31, §3, il permet à la CPVP d'adopter des recommandations qui font suite à une procédure de conciliation durant laquelle les droits de la défense doivent être respectés.

Dès lors, à notre sens, la CPVP ne devrait pas se prononcer sur la légalité des pratiques d'un responsable de traitement sans permettre à celui-ci de faire valoir son point de vue au préalable. Concrètement, lorsqu'elle reçoit un courrier qui vise les pratiques d'un responsable de traitement en particulier sans mentionner explicitement qu'il s'agit d'une plainte, la CPVP pourrait formuler deux types de réponses, en fonction de la manière dont le courrier est rédigé.

[1607] Art. 24 du règlement d'ordre intérieur de la CPVP, pris en application de l'art. 26, §1, 2e al., de la loi du 8 décembre 1992.

Soit, par son courrier, la personne semble s'informer, en demandant l'avis de la CPVP sur la légalité des pratiques d'un responsable de traitement. Dans ce cas, la CPVP pourrait analyser cette problématique dans le cadre de sa compétence générale de contrôle et d'inspection[1608]. La CPVP pourrait en aviser l'auteur du courrier, en précisant qu'elle l'informera de l'avis ou de la recommandation qui serait prise dans ce dossier, le cas échéant. Elle pourrait également rappeler à la personne l'existence de la procédure de plainte et les conditions liées à celle-ci.

Soit le courrier adressé à la CPVP fait davantage apparaître une dénonciation des agissements d'un responsable de traitement, plutôt qu'une simple demande d'informations. Dans ce cas, la CPVP pourrait contacter l'auteur de la lettre, pour lui demander si son courrier peut être qualifié de plainte. Dans l'affirmative, la CPVP devrait vérifier que la personne justifie d'un intérêt. La CPVP serait ensuite tenue de respecter la procédure de plainte organisée à l'article 31 de la loi du 8 décembre 1992.

Cette méthode permettrait à la CPVP de donner une suite utile aux courriers que lui adressent les citoyens tout en respectant les droits de la défense du responsable de traitement dont la légalité des pratiques est mise en cause.

III. Le recours « comme en référé » devant le Tribunal de première instance

480.- L'article 14 de la loi du 8 décembre 1992. Un citoyen mécontent qu'une administration refuse de lui communiquer les données à caractère personnel détenues à son sujet, ou rejette sa demande de rectification, d'opposition ou d'interdiction, peut assigner celle-ci devant le président du tribunal de première instance siégeant comme en référé.

> L'article 14 de la loi du 8 décembre 1992 prévoit que cette procédure peut être enclenchée pour « toute demande relative à la *communication* des données à caractère personnel » ainsi que « toute demande qui tend à *faire rectifier, supprimer ou interdire d'utiliser* toute données à caractère personnel d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne concernée s'est opposée ou encore qui a été conservée au-delà de la période autorisée »[1609].

[1608] À ce sujet, voy. les art. 37 à 40 du règlement d'ordre intérieur de la CPVP.
[1609] C'est nous qui soulignons.

Le recours organisé par l'article 14 de la loi du 8 décembre 1992 a fait l'objet de plusieurs commentaires en doctrine qui détaillent les difficultés nombreuses d'interprétation qu'elle suscite[1610]. Nous y renvoyons le lecteur et nous nous concentrons, dans les lignes qui suivent, sur les questions relatives à cette procédure qui sont directement liées à l'e-gouvernement.

A. L'utilité du recours

481.- Une voie plus efficace que le recours au Conseil d'État. Le chapitre précédent a montré que le recours au Conseil d'État présente trois difficultés majeures pour un citoyen désireux de protéger ses données à caractère personnel.

Premièrement, le recours en annulation et en suspension devant la section du contentieux administratif du Conseil d'État est conditionné au fait que l'acte attaqué soit un acte administratif au sens de l'article 14 des Lois coordonnées sur le Conseil d'État. Or, si l'on peut admettre que la décision par laquelle une administration refuse l'accès d'un citoyen à ses données à caractère personnel revêt cette qualité, il n'en va pas de même d'une décision de transfert de données qui s'apparente davantage à une mesure préparatoire d'un acte administratif[1611]. Deuxièmement, le Conseil d'État ne peut condamner l'administration à s'exécuter en nature. Il lui revient seulement d'annuler l'acte administratif, à charge pour le citoyen d'entamer à nouveau ses démarches dans l'espoir que l'administration adopte une nouvelle décision qui fasse droit à sa demande[1612]. Troisièmement, la procédure à suivre devant le Conseil d'État est longue et complexe[1613].

La procédure prévue par l'article 14 de la loi du 8 décembre 1992 présente donc un intérêt particulier dans l'e-gouvernement, pour plusieurs raisons.

Tout d'abord, cette procédure permet au citoyen de contourner les écueils du droit administratif traditionnel. En effet, la procédure n'est pas limitée à la contestation des actes administratifs.

[1610] Th. Leonard, « Observations », note sous Civ. Bruxelles (prés.), 22 mars 1994, *J.T.*, 1994, pp. 843 à 853 ; J Herveg, « La procédure 'comme en référé' appliquée aux traitements de données », *in Les actions en cessation,* Collection CUP, Bruxelles, Larcier, 2006, pp. 215 à 246 ; D. De Bot, *Verwerking van persoonsgegevens*, Anvers, Kluwer, pp. 352 et s.

[1611] Voy. *supra,* n° 443.-

[1612] Article 14 des Lois coordonnées sur le Conseil d'État. Voy. not., D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.,* pp. 291 et s.

[1613] À ce sujet, voy. D. Renders, T. Bombois, B. Gors, C. Thiebaut et L. Vansnick, *op. cit.,* pp. 256 et s.

En outre, cette procédure est rapide. Contrairement à la procédure « en référé », la procédure « comme en référé » ne nécessite pas que le demandeur prouve l'urgence. Celle-ci est présumée. Mais, comme la procédure « en référé », la procédure « comme en référé » est une procédure accélérée. Par ailleurs, l'ordonnance rendue par le président possède l'autorité de la chose jugée, car le juge exerce une compétence de fond. Elle est néanmoins exécutoire par provision, sans que le juge doive le préciser expressément[1614].

Enfin, la procédure « comme en référé » permet au juge judiciaire de condamner l'administration à s'exécuter en nature. Ainsi, si une administration ne répond pas à la demande d'accès d'une personne, le président du tribunal de première instance peut condamner l'administration à répondre à la demande d'accès qui lui a été faite, et assortir éventuellement cette injonction d'une astreinte. En outre, dans l'hypothèse où une administration répondrait à la demande du citoyen mais prétendrait ne pas disposer de données à caractère personnel à son sujet, le président du tribunal de première instance pourrait désigner un expert[1615]. Par ailleurs, toute personne intéressée peut également saisir le président du tribunal de première instance siégeant comme en référé dans le but d'obtenir la cessation immédiate des traitements de données interdits ou la suppression des données détenues illégalement par l'administration.

B. La difficulté d'exercer le recours dans l'e-gouvernement

482.- La mise en œuvre du recours. Des difficultés semblables à celles évoquées à propos de l'exercice du droit de rectification et d'interdiction font craindre que ce recours soit, lui aussi, mal adapté à l'e-gouvernement. En effet, pour être incitée à exercer ce recours, la personne intéressée doit avoir connaissance des traitements de données qui la concernent et des règles de protection des données qui s'y appliquent, afin de cerner les traitements de données problématiques. Elle doit également identifier le responsable du traitement afin de l'assigner. Par ailleurs, la matière est d'une telle technicité que l'intervention d'un avocat spécialisé sera le plus souvent nécessaire, entraînant des coûts non négligeables. Il faut encore compter sur des contraintes de procédure chronophages, telle que la comparution à une audience fixée par le juge.

[1614] Th. LEONARD, « Observations », *op. cit.,* p. 844 et les références citées.
[1615] *Ibid.,* p. 845 et références citées.

Ces facteurs sont d'autant plus décourageants que les juges eux-mêmes semblent souvent déroutés par la matière, ce qui peut avoir des conséquences sur les chances de réussite du recours.

> Par exemple, un traitement de données pourrait sembler interdit mais avoir néanmoins été autorisé par un comité sectoriel[1616], et/ou avoir reçu un avis favorable de la part de la CPVP[1617], ce qui n'est pas un cas d'école à l'heure où l'on s'interroge sur l'indépendance de l'autorité de contrôle des traitements de données. Dans quelle mesure le juge osera-t-il se détourner de ces documents, même s'ils ne s'imposent pas à lui ?

483.- La cause du recours. Le recours ne peut concerner que les données à caractère personnel de la personne concernée. On ne pourrait, par cette voie, contester un outil de traitement des données dans son ensemble, fût-il illégal.

> Ainsi, à notre sens, un citoyen pourrait obtenir l'interdiction du traitement de ses propres données par le système OASIS, mais pas la cessation du système lui-même.
>
> Dans le même sens, une personne intéressée pourrait contester le fait que la Banque-Carrefour de la sécurité sociale ne lui fournisse pas de copie de l'extrait du répertoire des références qui la concerne directement, mais elle ne pourrait contester par cette voie le fait que la Banque-Carrefour refuse – comme c'est effectivement le cas[1618]- de fournir le panorama général de l'emplacement des données à caractère personnel au sein des sources authentiques du réseau de la sécurité sociale.

484.- L'effet du recours. À l'issue de ce recours, le président du tribunal de première instance peut condamner le responsable du traitement à donner suite à la demande du citoyen concernant l'accès à ses données, ou à leur rectification, leur suppression ou leur interdiction d'utilisation. Si des données ont été communiquées à des tiers, le responsable du traitement peut également être condamné à avertir ces derniers de la rectification ou de la suppression des données.

Par contre, le juge du tribunal de première instance ne pourrait octroyer des dommages et intérêts au demandeur. Pour obtenir une telle indemnisation, la personne concernée doit introduire une demande de réparation conformément au droit commun[1619].

[1616] Voy. *infra,* n° 534.-

[1617] Voy. *infra,* n° 525.- et s.

[1618] Voy. *supra,* n° 299.-

[1619] À ce sujet, voy. J. Herveg, *op. cit.,* pp. 19 et 20 et les nombreuses references doctrinales et jurisprudentielles citées à la note 129.

IV. L'action en réparation

485.- Une responsabilité quais-objective. L'article 15*bis* de la loi du 8 décembre 1992 organise un régime de responsabilité sévère pour le responsable du traitement. En effet, si le responsable du traitement viole la loi du 8 décembre 1992 et, ce faisant, cause un dommage, la victime peut obtenir la réparation du dommage subi. Il lui suffit de prouver la réalité du dommage, l'existence d'un lien causal entre ce dommage et un traitement de données effectué par le responsable du traitement et, enfin, l'illégalité de ce traitement de données.

> L'article 15*bis* de la loi du 8 décembre 1992 est formulé en ces termes : « Lorsque la personne concernée subit un dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi, les alinéas 2 et 3 ci-après s'appliquent, sans préjudice d'actions fondées sur d'autres dispositions légales.
>
> Le responsable du traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi.
>
> Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable ».
>
> Cette disposition a été insérée dans la loi du 8 décembre 1992 l'occasion de la transposition, en 1998, de la directive 95/46. L'article 15*bis* de la loi du 8 décembre 1992 transpose dans l'ordre interne l'article 23 de la directive 95/46 qui, sous un intitulé « responsabilité », prévoit que « 1. Les États membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi. 2. Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable ».
>
> Remarquons que l'article 23 de la directive 95/46 est repris à l'article 77 de la proposition de règlement européen sur la protection des données.

L'article 15*bis* de la loi du 8 décembre 1992 consacre donc l'identité entre l'illégalité et la faute en matière de traitements de données à caractère personnel. En effet, dès le moment où la violation de la loi du 8 décembre 1992 cause un dommage à une personne, l'auteur de l'illégalité doit réparer ce dommage, sans qu'il faille apprécier le comportement du responsable du traitement par rapport à la situation dans laquelle il était placé au moment de commettre le fait dommageable. Cela revient à constater objectivement que la loi du 8 décembre 1992 a été violée, et à

en déduire automatiquement l'existence d'une faute dans le chef du responsable du traitement. Ce faisant, l'article 15*bis* de la loi du 8 décembre 1992 consacre un régime de responsabilité quasi-objective, sensiblement plus sévère que le régime de responsabilité de droit commun organisé par l'article 1382 du Code civil.

Remarquons que l'article 15*bis* de la loi du 8 décembre 1992 confère une valeur législative à la solution jurisprudentielle dégagée par la Cour de cassation en ce qui concerne la responsabilité des pouvoirs publics. Dans nos réflexions à ce sujet[1620], on a souligné que ce régime de responsabilité est avantageux pour les citoyens, mais sévère pour l'administration. Il est donc nécessaire que le législateur clarifie les règles applicables en la matière, afin que l'administration distingue plus aisément la frontière entre la légalité et l'illégalité en matière de traitements de données à caractère personnel.

486.- L'exonération de responsabilité. En vertu de l'article 15*bis* de la loi du 8 décembre 1992, l'administration peut s'exonérer de sa responsabilité en prouvant que l'illégalité qui a causé le dommage ne lui est pas imputable.

Dans l'e-gouvernement qui se caractérise, rappelons-le, par la collecte indirecte des données, cette cause d'exonération est intéressante pour l'administration à qui l'on reprocherait d'avoir pris une décision à partir de données fausses alors que ces données lui ont été communiquées par une autre administration. L'administration assignée en justice pourrait s'exonérer de sa responsabilité en identifiant l'origine des données et l'administration qui a commis l'erreur.

> Pour reprendre un exemple dont il a déjà été question, le SPF Economie décide d'octroyer, ou non, l'allocation de chauffage notamment à partir d'une donnée communiquée par le SPF Finances relative au revenu de la personne concernée. Imaginons que le SPF Finances communique au SPF Economie une donnée fausse qui indique que la personne concernée est au-dessus du seuil requis pour pouvoir bénéficier de ladite allocation, alors qu'en réalité, ses revenus sont inférieurs à ce seuil. Le SPF Economie refusera d'octroyer l'allocation de chauffage. Cette décision sera erronée. On pourrait alors reprocher au SPF Economie d'avoir violé l'article 4, 4°, de la loi du 8 décembre 1992 en prenant une décision à partir de données qui ne sont pas exactes. Cette illégalité reprochée au SPF Economie entraîne, en principe, l'obligation pour celui-ci d'indemniser la personne concernée du dommage qu'elle aurait subi en ne percevant pas à temps l'allocation de chauffage à laquelle elle a droit. Cependant, le SPF Economie pourrait s'exonérer de sa

[1620] Voy. *infra,* n° 456.- et s.

responsabilité en démontrant que la donnée relative au revenu lui a été communiquée par le SPF Finances et que l'erreur commise par le SPF Finances est la cause du dommage : sans cette erreur, le SPF Economie aurait attribué l'allocation de chauffage et la personne concernée n'aurait pas subi de dommage.

Section 2. Le contrôle par la CPVP

487.- L'historique de la CPVP. Le régime de la protection des données à caractère personnel impose l'existence d'une entité nouvelle dans le paysage institutionnel belge, la Commission de la protection de la vie privée (ci-après, « CPVP »).

À l'origine, la CPVP, dénommée alors « Commission consultative de la protection de la vie privée »[1621], est créée pour contrôler le respect de la première loi organisant le traitement de certaines données à caractère personnel, la loi du 8 août 1983 sur le Registre national. Elle rend des avis relatifs aux arrêtés royaux organisant l'accès au Registre national et l'utilisation du numéro d'identification au Registre national. En 1990, l'autorité de protection des données, désormais appelée « Commission de la protection de la vie privée », devient compétente pour surveiller également la Banque-carrefour de la sécurité sociale nouvellement instituée. Dès l'adoption de la loi du 8 décembre 1992, les normes régissant le statut et la compétence de la CPVP y sont intégrées.

À cette époque, la CPVP est instituée auprès du Ministère de la justice[1622], compétent en matière de protection de la vie privée[1623]. La CPVP collabore avec le Ministre, à qui elle remet copie de ses avis et de ses recommandations pour qu'il soit « informé des problèmes qui se poseront dans la pratique et puisse suivre de très près la jurisprudence de la Commission »[1624]. L'autorité de protection des données a, par ailleurs, « l'obligation de déposer un rapport annuel devant le Parlement qui retrouve ainsi *in fine* sa compétence de contrôle »[1625]. On souhaite néanmoins que

[1621] Art. 12 de la loi du 8 août 1983 organisant un registre national des personnes physiques, *Pasin.,*1983, II, p. 44.

[1622] Art. 23 de la loi du 8 décembre 1992 dans sa version initiale.

[1623] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, *op. cit.*, n° 1610/1, p. 29.

[1624] *Idem.*

[1625] Rapport du 27 octobre 1992 concernant le projet de loi relatif à la protection de la vie privée à l'égard des traitement de données à caractère personnel, fait au nom de la Commission de la justice par M. VANDENBERGHE, *Doc. parl.,* Sénat, sess. 1992-1993, pp. 47-48.

la CPVP soit indépendante, ce qui explique qu'elle est financée par un fonds spécial créé auprès du Ministère de la justice. En ce qui concerne les pouvoirs de la CPVP, celle-ci n'a alors qu'une compétence consultative qui prend la forme d'avis et de recommandations[1626].

En 2003, une importante réforme législative modifie le statut et les pouvoirs de la CPVP. Cette réforme est justifiée par le fait que la CPVP est surchargée et n'est plus en mesure d'exercer correctement ses missions[1627]. De plus, la protection des données à caractère personnel s'internationalise et force la présence de la CPVP dans diverses instances internationales[1628]. La loi du 26 février 2003[1629] entend répondre à ces difficultés. Outre le fait que les moyens humains à disposition de la CPVP sont renforcés[1630], la loi du 26 février 2003 modifie de manière importante le statut et les pouvoirs de la CPVP.

En ce qui concerne le statut de la CPVP, la loi du 26 février 2003 sort cette autorité du giron du pouvoir exécutif et la place auprès de la Chambre des représentants[1631]. Il ressort des travaux préparatoires que, ce faisant, le législateur a voulu faire de la CPVP un « organe collatéral de la Chambre

[1626] Pour de plus amples développements à ce sujet, voy. Y. POULLET, *op. cit.,* p. 77.

[1627] Ces difficultés s'expliquent par le fait que les traitements de données que la CPVP doit contrôler se multiplient à la faveur des évolutions technologiques. Ils touchent aux domaines les plus divers, qu'il s'agisse de l'efficacité administrative, de la gestion de la santé, de la surveillance des citoyens, du contrôle des travailleurs, ce qui requiert une large expertise de la part de la CPVP. En outre, les questions soulevées sont, le plus souvent, liées aux évolutions technologiques. Des particularités techniques doivent dès lors être maîtrisées pour saisir pleinement les dangers que les outils nouveaux présentent pour les citoyens. Par ailleurs, les citoyens sont de plus en plus conscients des traitements de leurs données. Ils sont ainsi portés à saisir davantage la CPVP pour obtenir réponse à leurs questions. Les autorités publiques le font également, soucieuses de mettre en œuvre correctement les normes particulièrement complexes qui régissent cette matière (Sur ces difficultés, voy. le plan de gestion de la CPVP disponible sur le site www. privacycommission.be, pp. 2 et 3).

[1628] E. DEGRAVE, « La CPVP : un organisme invincible ? », *R.D.T.I.,* 2006, pp. 227 et 228 ; D. DE BOT, « De Commissie voor de Bescherming van de Persoonlijke Levensfeer : 'Tussen droom en daad staan er niet alleen wetten in de weg, maar vooral praktische problemen'», *R.G.D.C.,* 2003, pp. 385-386.

[1629] Loi du 26 février 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *M.B.,* 26 juin 2003.

[1630] Art. 3 et 4 de la loi du 26 février 2003 précitée.

[1631] Voy. l'art. 23 de la loi du 8 décembre 1992 qui dispose qu' « il est institué auprès de la Chambre des représentants une Commission de la protection de la vie privée, composée de membres désignés par la Chambre des représentants, parmi lesquels le président et le vice-président ».

des représentants », ce qui lui « paraît plus logique »[1632] eu égard « à la mission de contrôle de l'administration qui lui incombe »[1633], bien qu'il reconnaisse qu'une telle « intégration [...] n'a, selon une étude de droit comparé, pas d'équivalent dans les pays voisins »[1634]. Les développements qui suivent montrent que cette modification n'est pas sans conséquence sur le contrôle juridictionnel de la CPVP qu'elle rend incertain[1635].

En outre, la loi du 26 février 2003 étend les pouvoirs de la CPVP. Elle crée, au sein de la CPVP, des comités sectoriels compétents pour autoriser ou interdire les traitements de données effectués dans un secteur particulier. En d'autres termes, depuis la loi du 26 février 2003, la CPVP dispose du pouvoir de prendre des décisions unilatérales et contraignantes à l'égard des tiers ce qui soulève la question de la recevabilité des recours introduits au Conseil d'État contre ces décisions[1636].

488.- La raison d'être de la CPVP. Trois critères sont souvent invoqués pour justifier la création d'autorités de protection des données[1637]. Ils ont guidé le législateur au moment de la mise en place de la CPVP[1638].

Ainsi, l'autorité de protection des données est composée de personnes faisant preuve d'une *expertise* dans les matières traitées, c'est-à-dire qu'elles ont une connaissance suffisante à l'égard de la protection des données à

[1632] Rapport fait au nom de la Commission de la justice par M. Tony Van Parys relatif à la proposition de loi « modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée », *op. cit.,* n° 50-1940/005, p. 4.

[1633] *Idem.*

[1634] *Ibid.*, p. 21. Voy. D. De Bot, *op. cit.,* pp. 387-389. Ce changement est amplement expliqué dans le chapitre consacré à l'indépendance de la Commission, *cf. infra.*

[1635] Voy. *infra,* n° 518.-

[1636] Voy. *infra,* n° 518.-

[1637] H. Mails, « Les autorités de contrôle et la défense de la vie privée », *in Vie privée : nouveaux risques et enjeux – Privacy : new risks and opportunities* (dir. Y. Poullet, C. de terwangne et P. Turner), Bruxelles, Éd. Story-Scientia, 1997, pp. 77 à 79. En ce sens, voy. Conseil d'État (France), *Rapport public 2001. Les autorités administratives indépendantes,* Études & Documents n° 52, p. 275. Ce rapport est disponible sur le site http://www.conseil-etat.fr/fr/rapports-et-Études/contributions.html

[1638] Pour la CPVP en particulier, voy. not. le projet de loi du 28 juin 1982 organisant un registre national des personnes physiques, *Doc. Parl.,* Ch. Repr., session 1982-1983, n° 296/1, p. 9 (« la Commission est composée d'experts qui sont reconnus pour leur compétence dans le domaine de l'informatique ») ; Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, *op. cit.,* n° 1610/1, p. 29 (« l'indépendance [de la CPVP] et les moyens dont elle disposera devraient lui permettre de jouer pleinement son rôle en la matière »).

caractère personnel et des technologies. Plusieurs spécialistes de ces questions sont d'ailleurs membres de la CPVP[1639].

L'*efficacité* de l'autorité de protection des données importe aussi, désignant la mesure dans laquelle l'action de cette institution permet d'atteindre l'objectif poursuivi qui est la protection de la vie privée des individus concernés. À cette fin, la CPVP est une autorité de régulation[1640] qui dispose de moyens d'action particuliers[1641].

Une dernière justification est l'*indépendance* de l'autorité de protection des données, à savoir, l'aptitude de l'institution à agir uniquement dans le but de protéger la vie privée des personnes concernées, sans se départir de ce but au profit d'autres intérêts. La CPVP est présentée comme une autorité indépendante[1642].

Les lignes qui suivent étudient, dans un premier temps, le statut de la CPVP. Cette dernière apparaît comme une autorité de régulation, soumise à une exigence d'indépendance. On s'interroge également sur la légitimité de la CPVP, pour savoir dans quelle mesure l'action de cette autorité indépendante se justifie dans notre société démocratique. Dans un deuxième temps, les moyens d'action de la CPVP sont analysés.

I. Le statut de la CPVP

489.- Une autorité de protection des données à caractère personnel[1643]**.** Comme son nom le laisse deviner, la CPVP est une autorité vouée spécifiquement à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Ainsi qu'on l'a déjà dit, cette autorité est née concomitamment à la création du Registre national, en 1983. Elle a ensuite été instituée et organisée par la loi du 8 décembre 1992[1644].

[1639] Voy. *infra,* n° 492.-

[1640] Voy. *infra,* n° 490.- et s.

[1641] Voy. *infra,* n° 523.- et s.

[1642] Voy. *infra,* n° 493.- et s.

[1643] Traditionnellement, le jargon de la protection des données désigne la CPVP et ses homologues étrangers tantôt par le vocable « autorité de contrôle des traitements de données à caractère personnel », tantôt par le vocable « autorité de protection des données à caractère personnel ». Nous choisissons d'utiliser cette deuxième acception dans le cadre de cette recherche.

[1644] Ce faisant, le législateur belge a devancé le prescrit des normes supranationales relatives à la protection de la vie privée et des données à caractère personnel. En effet, l'obligation d'instituer un tel organe de contrôle a été ancrée dans la directive 95/46 depuis son adoption en 1995, et dans la Convention 108 depuis une modification intervenue en 2001.

Les normes supranationales imposent aujourd'hui que chaque État crée une autorité de contrôle spécifiquement vouée à la protection des données à caractère personnel. Cette institution est d'ailleurs présentée comme un élément essentiel de la protection des données à caractère personnel des citoyens.

> Le considérant 62 de la directive 95/46 affirme que « l'institution, dans les États membres d'autorités de contrôle exerçant en toute indépendance leurs fonctions est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel ».
>
> Dans le même sens, le Préambule du Protocole additionnel à la Convention 108, adopté le 8 novembre 2001, souligne que « des autorités de contrôle exerçant leur fonction en toute indépendance sont un élément de la protection effective des personnes à l'égard du traitement des données à caractère personnel ».

A. Une autorité de régulation

490.- La notion de régulation et d'autorité de régulation. Une autorité de régulation est une institution spécifiquement vouée à la régulation d'un secteur déterminé. En général, cette qualification est attribuée aux autorités qui régulent un secteur économique, ce qu'elles font notamment en stimulant la concurrence entre différents opérateurs. C'est le cas, par exemple, de l'IBPT[1645] en matière de télécommunications, du CSA[1646] dans le domaine de l'audiovisuel, et de la CREG[1647] dans le domaine de l'énergie (gaz et électricité)[1648].

Il serait toutefois réducteur, au regard de la notion de régulation, de considérer qu'il n'existe d'autorité de régulation que dans le secteur

[1645] Institut belge des services postaux et des télécommunications.

[1646] Conseil supérieur de l'audiovisuel.

[1647] Commission de Régulation de l'Électricité et du Gaz.

[1648] Au sujet de ces autorités de régulation et pour d'autres exemples d'autorité de régulation dans le secteur économique, voy. not., D. De Roy et R. Queck, « De la téléphonie vocale aux offres publiques d'acquisition – Vers un 'droit de la régulation' ? », *J.T.,* 2003, pp. 556 et s. ; T. Hennen et N. Petit, « Les autorités de régulation de la concurrence », *T.B.H.,* 2007, pp. 529 et 533 et s. ; P. Boucquey et P.-O. de Broux, « Les recours juridictionnels contre les décisions des autorités de régulation », *La protection juridictionnelle du citoyen face à l'administration* (dir. H. Dumont, P. Jadoul et S. van Drooghenbroeck), Bruxelles, La Charte, 2007, pp. 215 et s. ; N. Petit, « The Proliferation of National Regulatory Authorities alongside Competition Authorities : A source of Jurisdictional Confusion ? », *in Regulation through Agencies-A new Paradigm of European Governance* (eds. D. Geradin, R. Munoz et N. Petit), Cheltentham, Edward Elgar, 2005, pp. 180 et s.

économique. En effet, la *régulation* est une notion large et d'ailleurs difficile à définir[1649]. Elle peut toutefois être appréhendée au travers du but que poursuit la régulation d'un secteur, et des moyens sur lesquelles elle se fonde. Ainsi, l'objectif de la régulation est d'assurer un équilibre entre des intérêts contradictoires, pour garantir le bon fonctionnement d'un secteur[1650]. Quant aux moyens mis en œuvre pour atteindre cet objectif, ils s'expliquent à partir du constat suivant : le secteur régulé présente la caractéristique d'être soumis à des « turbulences incessantes que provoquent des évolutions technologiques rapides et imprévisibles, ou des conjonctures économiques particulières »[1651]. Dans ce contexte, « l'État est [...] dépassé par la tâche » [1652]; les normes générales et abstraites adoptées par le pouvoir législatif et le pouvoir exécutif ne suffisent plus à elles seules pour garantir l'objectif d'équilibre dans le secteur en question. Ces normes doivent donc être complétées par des moyens individuels et concrets, souples et adéquats.

Les autorités de régulation répondent à ce besoin en régulant « aux confins de l'État et de la société civile, des secteurs qu'on ne se résout pas à laisser aux seules forces du marché, tout en ne pouvant plus les maintenir sous la coupe exclusive des pouvoirs publics »[1653]. Par leurs décisions, les autorités de régulation ajustent, au cas par cas, « les rapports entre forces contraires, comme l'horloger qui veille avec doigté au mouvement du balancier »[1654]. Elles le font grâce à des moyens d'action diversifiés parmi lesquels certains se rapprochent des moyens juridiques classiques – on pense au pouvoir de sanction et au pouvoir d'agir en justice, par exemple. D'autres sont plus souples et davantage fondés sur la concertation – tels que les avis, les recommandations, les conciliations, les rapports[1655].

L'institution d'une autorité de régulation présente également d'autres avantages[1656]. Grâce à cette autorité, la régulation du secteur n'est pas lais-

---

[1649] Différentes définitions sont proposées par M.-A. Frison-Roche, « Les différentes définitions de la régulation », *Petites affiches,* 10 juillet 1998, p. 5.

[1650] M.-A. Frison-Roche, « Le droit de la régulation », *D.,* 2001, p. 613 ; D. De Roy et R. Queck, *op. cit.*, p. 555.

[1651] D. De Roy et R. Queck, *op. cit.*, p. 555.

[1652] M.-A. Frison-Roche, « Le droit de la régulation », *op. cit.,* p. 612.

[1653] F. Ost, « La régulation : des horloges et des nuages », *in Elaborer la loi aujourd'hui, mission impossible ?* (dir. B. Jadot et F. Ost), Bruxelles, Publications des Facultés universitaires Saint-Louis, p. 21.

[1654] D. De Roy et R. Queck, *op. cit.*, pp. 556.

[1655] X. Delgrange, L. Detroux et H. Dumont, « La régulation en droit public », *in Elaborer la loi aujourd'hui, mission impossible ?* (dir. B. Jadot et F. Ost), *op. cit.,* pp. 71 et 72.

[1656] X. Delgrange, L. Detroux et H. Dumont, « La régulation en droit public », *in Elaborer la loi aujourd'hui, mission impossible ?* (dir. B. Jadot et F. Ost), *op. cit.,* p. 71.

sée exclusivement aux mains de l'État. C'est particulièrement intéressant dans les domaines où des droits fondamentaux sont en jeu et qu'il convient de veiller à ce que l'autorité étatique les respecte. Par ailleurs, l'autorité de régulation peut être composée d'individus qui sont tout à la fois spécialisés dans les matières du secteur régulé et indépendants par rapport à celui-ci. Cela renforce la qualité des solutions proposées et leur adéquation par rapport aux problématiques à réguler.

491.- La CPVP est une autorité de régulation. L'ensemble formé par les traitements de données à caractère personnel peut être considéré comme un secteur. En effet, au même titre que l'énergie ou les télécommunications, les traitements de données constituent « un regroupement d'activités ayant certains caractéristiques communes »[1657].

Ce secteur présente des caractéristiques qui expliquent que les normes générales et abstraites émanant des pouvoirs législatif et exécutif ne suffisent pas pour le réguler. D'une part, les traitements de données ne peuvent pas tous être anticipés et définis *a priori* dans une norme. Le premier titre de la recherche a montré, en effet, qu'il est déjà très difficile pour le législateur de définir les éléments essentiels des traitements de données. On ne pourrait exiger de lui qu'il organise chaque traitement de données, ce qui nuirait d'ailleurs à la lisibilité des normes. C'est pourquoi, le contrôle de la légalité des traitements de données doit pouvoir être soumis à un examen au cas par cas. D'autre part, les traitements de données évoluent avec les technologies, et cette évolution est rapide. Elle fait naître régulièrement de nouvelles questions, au gré des nouveaux outils de traitement qui sont créés. Celles-ci appellent une réponse rapide.

La CPVP est instituée en tant qu'autorité de régulation du secteur formé par les traitements de données à caractère personnel. Son rôle est important à différents égards.

Tout d'abord, son travail complète l'arsenal législatif et réglementaire qui n'est pas suffisant pour encadrer tous les traitements de données réalisés dans l'administration.

En outre, l'existence de la CPVP évite que la régulation de l'e-gouvernement soit laissée exclusivement aux mains de l'État. Elle permet également de contrôler l'État. C'est particulièrement important en matière d'e-gouvernement car si le législateur et le Gouvernement décidaient seuls des solutions appliquées en ce domaine, on pourrait craindre que trop d'attention soit accordée à l'efficacité administrative, au détriment de la protection de la vie privée des citoyens. En effet, comme le

[1657] Définition du terme « secteur » dans le Dictionnaire *Le Robert*.

constataient déjà certains auteurs dans les années septante, ce qui importe, « c'est d'empêcher le mauvais usage de l'ordinateur. Mais qui va définir le bon et le mauvais usage ? Le pouvoir d'État. Et qui est le plus susceptible de faire un mauvais usage ? Le pouvoir d'État »[1658]. Cela explique que l'autorité de protection des données doit faire preuve d'une grande indépendance à l'égard de l'État[1659].

Enfin, ainsi que nous le verrons, la CPVP est composées d'*experts*, ce qui est appréciable compte tenu de la technicité des questions soulevées par les traitements de données à caractère personnel. Les membres de la CPVP doivent également être indépendants ce qui, en pratique, n'est pas toujours le cas, comme nous le verrons.

Pour accomplir ses missions, la CPVP dispose d'un certain nombre de moyens d'action orientés vers un objectif commun, celui de trouver, au gré des questions dont elle doit connaître, un équilibre entre l'intérêt du responsable du traitement de données et le droit à la protection de la vie privée de la personne dont les données sont traitées. Dans l'e-gouvernement en particulier, la CPVP définit ce délicat équilibre en mettant en balance l'efficacité administrative, d'une part, et la protection de la vie privée des citoyens, d'autre part. Elle rend alors un avis qui approuve ou, au contraire, désapprouve une législation mettant en place un nouvel outil de traitements de données au sein de l'administration, ou émet une recommandation à l'égard d'un responsable de traitement qui violerait la loi du 8 décembre 1992, ou encore autorise ou interdit, par l'intermédiaire d'un comité sectoriel, un échange de données entre deux administrations, etc.

492.- La composition de la CPVP. La CPVP regroupe trois entités distinctes, à savoir la Commission, les comités sectoriels et le secrétariat.

a) La Commission. En vertu de l'article 24 de la loi du 8 décembre 1992, la Commission se compose de seize membres. Ceux-ci sont désignés pour un terme de six ans renouvelable. Tous doivent présenter les garanties nécessaires pour exercer leur travail en toute indépendance.

> C'est la raison pour laquelle, notamment, ledit article 24 prévoit que les membres de la Commission ne peuvent être membre du Parlement européen ou des Chambres législatives, ni d'un Parlement de communauté ou de région.

[1658] J.-L. Missika et J.-P. Faivret, « Informatique et libertés », *Les temps modernes,* 1977, n° 375, p. 314.

[1659] Voy. *infra,* n° 493.- et s.

Tous doivent également, selon les termes dudit article 24, être « parfaitement compétents dans le domaine de la protection des données ».

> Parmi les seize membres figurent au moins un juriste, un informaticien, une personne pouvant justifier d'une expérience professionnelle dans la gestion de données à caractère personnel relevant du secteur privé, et une personne pouvant justifier d'une expérience professionnelle dans la gestion de données à caractère personnel relevant du secteur public.

À la tête de ces seize membres, se trouve un président, qui doit être magistrat. Il est épaulé par un vice-président. Leur langue maternelle doit obligatoirement différer. Ils exercent leur fonction à temps plein.

Aux côtés du président et du vice-président, se trouvent six membres effectifs et huit membres suppléants. Ils ne travaillent pas à temps plein auprès de la Commission et sont seulement tenus d'être présents aux séances qui ont lieu toutes les trois semaines[1660].

b) Les comités sectoriels. Les comités sectoriels sont créés à partir du modèle du comité de surveillance de la Banque-Carrefour de la sécurité sociale. Cette autorité sectorielle a été instituée par la loi du 15 janvier 1991, aux fins de contrôler les traitements de données dans le secteur de la sécurité sociale. Dans les années qui suivent, le législateur souhaite multiplier les autorités sectorielles du genre, en créant notamment un comité d'autorisation de la Banque-Carrefour des Entreprises et un Comité d'habilitation pour le Registre national[1661].

Néanmoins, la création éparse de ces organes risque d'entraîner « un éclatement [...] du niveau de protection en matière de transfert de données » ainsi que « des dépenses de fonctionnement non négligeables »[1662]. Dès lors, à l'occasion des réflexions menées préalablement à l'adoption de la loi du 26 février 2003, il apparaît judicieux d'intégrer ces autorités sectorielles à la structure de la CPVP. On affirme qu'« une telle solution est assurément de nature, en bref, à assurer une cohérence dans le niveau de

---

[1660] Comme le précise le site de la CPVP www.privacycommission.be rubrique Commission – organisation.

[1661] Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.*, n° 50-1940/001, p. 7.

[1662] Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.*, n° 50-1940/001, pp. 6, 7 et 9.

protection des données, une facilité renforcée d'accès du citoyen en vue de la protection de ses droits ainsi qu'une utilisation plus rationnelle des deniers publics »[1663].

Depuis la réforme législative intervenue en 2003, existent, au sein de la CPVP, le comité sectoriel de la sécurité sociale et de la santé[1664], le comité sectoriel de la Banque-Carrefour des Entreprises[1665], le comité sectoriel du Registre national[1666], le comité sectoriel de l'Autorité Fédérale[1667], le comité de surveillance sectoriel « Phenix » dans le secteur judiciaire[1668], et le comité de surveillance statistique[1669], en attendant la création d'autres comités[1670]. Ils sont institués au sein de la CPVP, en vertu de l'article 31 *bis* de la loi du 8 décembre 1992, et veillent au respect de la protection de la vie privée lors des traitements de données à caractère personnel qui ont lieu dans le secteur dont ils relèvent.

Chaque comité sectoriel est composé de six membres effectifs et six membres suppléants, désignés pour un mandat renouvelable de six ans[1671]. La moitié des membres des comités sectoriels sont issus de la CPVP et

---

[1663] Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.*, n° 50-1940/001, p. 9.

[1664] Art. 37 à 52 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale. Voy. D. De Bot, *op. cit.,* p. 399.

[1665] Art. 27 à 32 de la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises [...] ; Arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP.

[1666] Art. 5 de la loi du 8 août 1983 organisant un registre national des personnes physiques ; Arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP.

[1667] Art. 36*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des données à caractère personnel ; Arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP.

[1668] Art. 22 à 26 et 28 de la loi du 10 août 2005 instituant le système d'information Phenix.

[1669] Art. 24*sexies* à 24*octies* de la loi du 4 juillet 1962 relative à la statistique publique, *M.B.,* 20 juillet 1962.

[1670] Ces autorités de contrôle sont étudiées dans le chapitre III du présent titre de la recherche.

[1671] Art. 31*bis,* §2, de la loi du 8 décembre 1992 ; art. 4 de l'arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP, *M.B.,* 30 décembre 2003. La présidence du comité sectoriel revient, en principe, au président de la CPVP. Celui-ci peut toutefois se désister, auquel cas, un des membres du comité sectoriel est désigné président.

l'autre moitié est constituée d'experts émanant du secteur concerné[1672]. Cette composition est censée répondre à l'exigence d'expertise dont l'autorité de protection des données doit faire preuve[1673].

> Par exemple, au sein du comité sectoriel de la Banque-Carrefour des entreprises, du comité sectoriel du Registre national et du comité sectoriel pour l'Autorité fédérale, les membres extérieurs à la CPVP peuvent se prévaloir d'une expertise juridique, d'une expérience professionnelle dans le domaine de l'utilisation des données à caractère personnel ou encore, d'une expérience en matière d'e-gouvernement ou de simplification administrative, comme l'impose l'arrêté royal qui règle la composition de ces comités sectoriels[1674].

Par ailleurs, chaque comité sectoriel ressortit d'une institution de gestion, dont la mission est assurée par un service public fédéral. La tâche de l'institution de gestion consiste essentiellement à transmettre au comité sectoriel un avis juridique et technique relatif à chaque demande d'autorisation de traitement de données qui lui parvient et ce, préalablement à la décision du comité sectoriel[1675]. L'institution de gestion est le Service public fédéral Economie, le Service public fédéral Intérieur, la Banque-Carrefour de la sécurité sociale ou le Service public fédéral des Technologies de l'information et des communications, suivant le type de données visé par la demande d'accès[1676].

[1672] Le comité sectoriel de la sécurité sociale et de la santé fait exception à ce mode d'organisation. Il est composé de deux sections : une section sécurité sociale et une section santé. Chaque section est composée de six membres. Deux membres sont issus de la Commission tandis que les autres sont des membres externes, principalement des médecins. En d'autres termes, sur les douze membres qui composent ce comité sectoriel, seuls quatre d'entre eux proviennent de la Commission.

[1673] Voy. *supra,* n° 488.-

[1674] Art. 3 de l'arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP, *M.B.,* 30 décembre 2003.

[1675] Art. 31*bis*, §3, de la loi du 8 décembre 1992. Voy. égal. *infra,* n° 573.-

[1676] Art. 2 de l'arrêté royal du 17 décembre 2003 précité ; art. 42 de la loi du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale.

Depuis leur intégration au sein de la CPVP, chaque comité sectoriel est établi, en principe[1677], au siège de cette dernière[1678]. Toutefois l'institution de gestion d'un comité sectoriel peut demander à la CPVP que le comité sectoriel dont elle relève siège à ses côtés, ce qui peut se justifier au regard de « considérations d'efficacité, d'optimalisation des relations avec l'institution contrôlée et de prise en compte de situations existantes »[1679].

c) Le secrétariat. L'article 35 de la loi du 8 décembre 1992 institue le secrétariat de la CPVP. Il s'agit d'une administration, composée d'agents de l'État. Elle offre une aide substantielle à la CPVP et aux comités sectoriels, notamment en préparant les dossiers à traiter, en distinguant les questions qui peuvent être réglées rapidement de celles qui nécessitent des recherches approfondies. Cette administration est organisée en cinq sections[1680] relevant chacune d'un chef de section.

B. Une autorité indépendante ?

493.- L'exigence d'indépendance. Tant la directive 95/46, que la Convention 108 et la loi du 8 décembre 1992 imposent que l'autorité de protection des données soit indépendante.

> L'article 28 de la directive 95/46 et l'article 1.3 du Protocole additionnel à la Convention 108 concernant les autorités de contrôle notamment, ne

[1677] Le Comité sectoriel de la sécurité sociale et de la santé fait exception à cette règle, au motif qu'au moment où les comités sectoriels ont été intégrés à la CPVP, le comité sectoriel de la sécurité sociale était le seul comité sectoriel existant. On a jugé nécessaire que « par rapport à ceux en cours d'institution (Banque-Carrefour des entreprises, registre national, etc.), il soit difficile de faire entièrement abstraction des règles actuelles de fonctionnement dudit comité. » (Rapport fait au nom de la Commission de la Justice par M. Tony Van Parys relatif à la proposition de loi « modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *Doc. Parl.*, Ch. Repr., sess. 2002-2003, n° 50-1940/005, p. 9).

[1678] Art. 31*bis*, §5, de la loi du 8 décembre 1992 ; art. 41 de la loi du 15 janvier 1990.

[1679] Rapport fait au nom de la Commission de la Justice par M. Tony Van Parys relatif à la proposition de loi « modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.*, n° 50-1940/005, p. 8.

[1680] Il s'agit de la Direction général, du Staff de la présidence, de la Section Organisation et Gestion des ressources, de la Section Études et Recherche, et de la Section Relations externes. Pour de plus amples détails, voy. le site de la Commission www.privacycommission.be rubrique Commission-secrétariat.

> disposent que les autorités de contrôle à l'égard des traitements de données à caractère personnel « exercent en toute indépendance » leurs missions.
>
> La loi du 8 décembre 1992 prévoit, depuis son adoption, que la CPVP œuvre de manière indépendante[1681].

La CPVP répond-t-elle à cette exigence ?

§1. La notion d'indépendance

494.- Pourquoi une exigence d'indépendance ? Par rapport à qui ? Et comment ? Ni la directive 95/46, ni le Protocole additionnel à la Convention 108, ni la loi du 8 décembre 1992 ne fournissent de critères permettant de cerner la notion d'indépendance applicable aux autorités de protection des données à caractère personnel. Dès lors, la compréhension de l'exigence d'indépendance suppose que l'on identifie sa raison d'être, que l'on s'interroge sur son étendue et qu'on en définisse les conditions. Il convient ensuite d'apprécier le respect de ces conditions par la CPVP.

1. La raison d'être de l'indépendance

495.- Objectivité et impartialité. Dans deux arrêts récents dont il sera encore question par la suite[1682], la Cour de justice de l'Union européenne interprète la portée de l'exigence d'indépendance des autorités de protection des données. Le premier arrêt concerne les autorités de protection des données instituées dans les *Länder* allemands[1683] tandis que le second vise l'autorité de protection des données autrichienne[1684].

[1681] Art. 23 de la loi du 8 décembre 1992 en sa version initiale ; art. 24, §4, de la loi du 8 décembre 1992 depuis sa modification par la loi du 26 février précitée.

[1682] Voy. *infra,* n° 497.- et s.

[1683] C.J.U.E., gde ch., 9 novembre 2010, *République fédérale d'Allemagne c. Commission,* C-518/07. Pour un commentaire de cet arrêt, voy. M. Aubert, E. Broussy et F. Donnat, « Chronique de jurisprudence communautaire », *AJDA,* 2010, pp. 938 et 939 ; H.R. Kranenborg, « Commentaar », *SEW,* 2010, pp. 421 à 423 ; E. Debaets, « Les autorités administratives indépendantes et le principe démocratique : recherches sur le concept d' 'indépendance' », Rapport présenté au VIIIème Congrès mondial de l'association internationale de droit constitutionnel, Mexico, 6-10 décembre 2010 disponible sur le site www.juridicas.unam.mx/wccl/ponencias/14/254.pdf ; European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* 7 mai 2010, p. 19, disponible sur le site www.fra.europa.eu ; O. De Schutter, « Les droits fondamentaux dans l'Union européenne », *J.D.E.,* 2011, pp. 113 et 114.

[1684] C.J.U.E., gde ch., 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10.

À cette occasion, elle se livre à une interprétation téléologique de la directive 95/46 et dégage la raison d'être de l'exigence d'indépendance. Ainsi, selon la Cour, l'indépendance de l'autorité de protection des données est imposée afin de permettre à cette dernière d'effectuer un examen objectif et impartial de l'équilibre à atteindre entre la circulation des données à caractère personnel et la protection de la vie privée des personnes concernées.

> Dans son premier arrêt, confirmé par le second arrêt, la Cour rappelle que l'objectif poursuivi par la directive européenne est d'assurer la libre circulation des données entre les États-membres. Puisque ces échanges d'informations peuvent heurter la vie privée des citoyens concernés, les autorités de contrôle doivent être des « gardiennes [des] droits et libertés fondamentaux »[1685]. Leur tâche revient à « assurer un juste équilibre entre, d'une part, le respect du droit fondamental à la vie privée et, d'autre part, les intérêts qui commandent une libre circulation des données à caractère personnel »[1686]. Partant de là, l'indépendance des autorités de contrôle s'entend des garanties permettant à ces institutions d'examiner cet équilibre « de manière objective et impartiale »[1687].

2. L'étendue de l'indépendance

496.- Une indépendance ample. Qui pourrait exercer sur l'autorité de protection des données une pression telle que l'examen précité ne pourrait être effectué de manière objective et impartiale ? En d'autres termes, de quelle sphère d'influence cherche-t-on à protéger l'autorité de protection des données en manifestant un tel souci d'indépendance ? Comme l'affirme David De Roy, « l'identification de la sphère d'influence est [...] délicate, car elle conduit à distinguer deux hypothèses entre lesquelles règne parfois une certaine confusion »[1688].

L'autorité de protection des données est instituée pour protéger le droit fondamental à la vie privée dans le secteur des traitements de données à caractère personnel. Son intervention peut également avoir un impact

[1685] C.J.U.E., gde ch., 9 novembre 2010, *République fédérale d'Allemagne c. Commission,* C-518/07, § 23.

[1686] *Ibid.,* § 24.

[1687] *Ibid.*, § 25. Dans le même sens, C.J.U.E., gde ch., 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10, §§ 40 et 41.

[1688] D. De Roy, « Le pouvoir réglementaire des autorités administratives indépendantes en droit belge », *op. cit.,* n° 17.

économique en favorisant la concurrence loyale entre des opérateurs privés désireux d'utiliser des données à caractère personnel[1689].

Les traitements de données étant effectués au sein du secteur privé et du secteur public, cette autorité contrôle un grand nombre d'organismes, dont les administrations. Dès lors, la CPVP est à la fois comme un relai de l'action étatique, lorsqu'elle contrôle le secteur privé, qu'un moyen de contrôle de l'État, s'agissant de l'examen de traitements de données effectués par les administrations[1690]. Le contrôle exercé par les comités sectoriels vise même principalement les administrations puisqu'ils peuvent empêcher une administration de communiquer les données qu'elle détient[1691]. C'est d'ailleurs pour renforcer le contrôle de la CPVP à l'égard de l'administration que cette autorité a été placée auprès de la Chambre des représentants par la réforme législative de 2003.

> Les discussions préparatoires à cette réforme législative affirment que « les compétences de la Chambre des représentants en matière de contrôle politique et en matière budgétaire, et plus généralement la place que lui reconnaît la Constitution, justifient que ce soit auprès d'elle que soit désormais placée la Commission »[1692], cette dernière ayant notamment une mission de « contrôle de l'administration »[1693].

Dès lors, étant donné que l'autorité de protection des données doit faire preuve d'objectivité et d'impartialité tant à l'égard des sociétés privées que

---

[1689] À ce sujet, voy. E. Degrave, « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données à caractère personnel illégal sanctionné par la Cour d'appel de Bruxelles », observations sous Bruxelles (9e ch.), 9 mai 2012, *J.T.*, 2012, pp. 691-693. Dans cette décision, la Cour d'appel de Bruxelles condamne une société privée qui utilise des données à caractère personnel en violant une interdiction d'un comité sectoriel. Le juge considère qu'il s'agit d'une illégalité, source de concurrence déloyale.

[1690] E. Debaets, « Les autorités administratives indépendantes et le principe démocratique : recherches sur le concept d' 'indépendance' », Rapport présenté au VIIIe Congrès mondial de l'association internationale de droit constitutionnel, Mexico, 6-10 décembre 2010 disponible sur le site www.juridicas.unam.mx/wccl/ponencias/14/254.pdf, p. 4.

[1691] Voy. *infra,* n° 534.-

[1692] Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.*, n° 50-1940/001, p. 10.

[1693] Rapport fait au nom de la Commission de la Justice par M. Tony Van Parys relatif à la proposition de loi « modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.,* n° 50-1940/005, p. 4.

de l'administration, il y a lieu de lui assurer une indépendance particulièrement ample.

497.- L'interprétation de la Cour de justice de l'Union européenne. La Cour de justice de l'Union européenne prône également une interprétation large de l'exigence d'indépendance dans les deux arrêts récents qui viennent d'être évoqués[1694]. La Cour soutient qu'étant donné que la directive 95/46 prescrit à l'autorité de protection des données d'agir en « toute » indépendance, cela signifie qu'elle doit « jouir d'une indépendance qui [lui] permette d'exercer [ses] missions sans influence extérieure ». Cela exclut « non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte, qui pourraient remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel »[1695].

Partant de là, elle juge que les autorités de protection des données allemandes ne sont pas indépendantes, étant donné qu'elles sont soumises à un contrôle de tutelle de l'État[1696].

L'autorité de protection des données autrichienne (la « DSK »[1697]) ne respecte pas non plus cette exigence d'indépendance et ce, pour trois raisons. Tout d'abord, le membre administrateur de la DSK, qui est un des six membres qui composent cette autorité et en gère les affaires courantes, est un fonctionnaire fédéral assujetti à un contrôle de tutelle. Ensuite, le bureau de la DSK est intégré aux services de la chancellerie fédérale, ce qui signifie que le personnel mis à la disposition de la DSK est composé de fonctionnaires de la chancellerie fédérale. Enfin, le chancelier fédéral a le droit inconditionnel d'être informé au sujet de tous les aspects de la gestion de la DSK[1698].

Une interprétation si large de l'exigence d'indépendance emporte des conséquences délicates pour la Belgique, s'agissant du contrôle des décisions prises par la CPVP[1699].

[1694] Voy. *supra,* n° 495.-

[1695] C.J.U.E., gde ch., 9 mars 2010, *République fédérale d'Allemagne c. Commission,* C-518/07 §30 ; C.J.U.E., gde ch., 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10, § 41.

[1696] C.J.U.E., gde ch., 9 mars 2010, *op. cit.*, §58.

[1697] DSK est l'abréviation de *Datenschutzkommission*.

[1698] C.J.U.E., gde ch., 16 octobre 2012, *République d'Autriche c. Commission, op. cit.*, § 66.

[1699] Voy., *infra,* n° 517.-

3. Les conditions de l'indépendance

498.- Plusieurs conditions. Le Rapport explicatif sur le protocole additionnel à la Convention 108[1700] énumère les critères d'indépendance de l'autorité de protection des données. Ceux-ci concernent tant les membres qui composent l'autorité, que l'autorité elle-même.

499.- L'indépendance des membres. L'indépendance de l'autorité de protection des données suppose avant tout l'indépendance de ses membres. On sera ainsi particulièrement attentif à la composition de l'autorité, au mode de désignation de ses membres, à la durée de leur mandat et aux conditions de cessation de leurs fonctions. À cet égard, rappelons[1701] que pour la Cour de justice de l'Union européenne, le fait que le membre administrateur de l'autorité de protection des données autrichienne soit un fonctionnaire fédéral et que le personnel mis à la disposition de cette autorité soit composé de fonctionnaires est contraire à l'exigence d'indépendance prescrite par la directive 95/46.

Un rapport de l'Agence des droits fondamentaux de l'Union européenne (FRA) affirme que l'indépendance des membres de l'autorité de protection des données est source de préoccupation dans beaucoup d'États européens compte tenu du risque d'influence du Gouvernement sur ces derniers. C'est pourquoi, une attention particulière doit être accordée au mode de désignation et de révocation de ces membres[1702].

> L'article 47 de la proposition de règlement général sur la protection des données, rédigé postérieurement à ce rapport, indique que « 3. Les membres de l'autorité de contrôle s'abstiennent de toute acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non ».
>
> En outre, l'article 48 de cette même proposition, qui porte sur les conditions générales applicables aux membres de l'autorité de contrôle, dispose notamment que « 1. Chaque État membre prévoit que les membres de l'autorité de contrôle doivent être nommés soit par son parlement soit par son Gouvernement. 2. Les membres sont choisis parmi les personnes offrants toutes garanties d'indépendance et qui possèdent une expérience et une compétence notoires dans l'accomplissement de leurs fonctions, notamment dans le domaine de la protection des données à caractère personnel ».

[1700] Rapport explicatif sur le protocole additionnel à la Convention 108, § 17.

[1701] Voy. *supra*, n° 497.-

[1702] European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* 7 mai 2010, p. 19, disponible sur le site www.fra.europa.eu.

500.- L'indépendance institutionnelle. L'indépendance institutionnelle de l'autorité de protection des données suppose l'octroi de ressources financières et matérielles suffisantes. Elle suppose également que l'autorité de protection des données ne soit pas soumise à des ordres ou des injonctions venant de l'extérieur. En ce sens, rappelons[1703] que la Cour de justice de l'Union européenne estime que la mise en place d'un contrôle de tutelle de l'État sur l'autorité de protection des données est contraire à l'exigence d'indépendance. Tel est le cas également si un ministre dispose d'un droit inconditionnel d'information qui s'exerce sur tous les aspects de la gestion de l'autorité de protection des données.

> L'article 47 de ladite proposition de règlement précise également l'exigence d'indépendance institutionnelle et prévoit que « 5. Chaque État membre veille à ce que l'autorité de contrôle dispose des ressources humaines, techniques et financières appropriées, ainsi que des locaux et de l'infrastructure, nécessaires à l'exécution effective de ses fonctions et pouvoirs, notamment ceux qu'elle doit mettre en œuvre dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité européen de la protection des données. 6. Chaque État membre veille à ce que l'autorité de contrôle dispose de son propre personnel, qui est désigné par le directeur de l'autorité de contrôle et est placé sous les ordres de celui-ci. 7. Les États membres veillent à ce que l'autorité de contrôle soit soumise à un contrôle financier qui ne menace pas son indépendance. Les États membres veillent à ce que l'autorité de contrôle dispose de budgets annuels propres. Les budgets sont rendus publics ».

§2. L'indépendance de la CPVP

501.- Considérations générales. L'organisation de la CPVP doit être confrontée à l'exigence d'indépendance telle qu'elle vient d'être développée. D'emblée, deux caractéristiques suscitent la réflexion, à savoir le mode de désignation des membres de la CPVP et son institution en tant qu'organe du pouvoir législatif après avoir fait partie du pouvoir exécutif.

1. L'indépendance des membres de la CPVP

502.- Considérations générales. L'indépendance de la CPVP pose question au regard du mode de désignation de ses membres et de la manière dont elle est composée.

[1703] Voy. *supra,* n° 497.-

503.- Le mode de désignation des membres de la CPVP.

a) Chambre des représentants et Conseil des ministres. Les membres de la CPVP sont élus par la Chambre des représentants sur des listes comprenant, pour chaque mandat à pourvoir, deux candidats présentés par le Conseil des ministres[1704].

> Dans son rapport sur les autorités chargées de la protection des données à caractère personnel, l'Agence des droits fondamentaux de l'Union européenne fait apparaître que l'élection des membres de l'autorité de protection des données par le Parlement – pratiquée également en Grèce, en Allemagne et en Slovénie – est un mécanisme de désignation bien plus respectueux de l'exigence d'indépendance que la nomination par le Gouvernement – comme en Irlande ou au Luxembourg – ou le rattachement de ladite autorité au Ministère de la justice – comme au Danemark ou en Lettonie et comme c'était le cas en Belgique avant la réforme de 2003[1705].

b) Les difficultés. Conformément à ce qu'a affirmé la Cour de justice de l'Union européenne, l'élection des membres par la Chambre des représentants n'est pas, en soi, une atteinte à l'indépendance de l'autorité de protection des données. Néanmoins, la présentation des candidats par le Conseil des ministres pose question. En effet, le pouvoir du Conseil des ministres de présenter deux candidats pour chaque poste à pourvoir limite le choix de la Chambre des représentants, en le teintant d'une logique majoritaire. La section de législation du Conseil d'État affirme ainsi que ce pouvoir est « inhabituel » et est « de nature à limiter sérieusement le choix des chambres législatives »[1706].

En outre, on peut raisonnablement penser que, concrètement, les candidats choisis par le Conseil des ministres émanent des cabinets ministériels et des administrations. Une fois membres de la CPVP, ces personnes sont appelées à contrôler l'action administrative. N'y a-t-il pas là un risque de manque d'impartialité dans l'exercice de leurs tâches[1707] ? C'est en ce

---

[1704] Art. 24, §1er, de la loi du 8 décembre 1992.

[1705] European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* précité, pp. 19-20.

[1706] SLCE du 28 novembre 1990 sur un projet de loi « relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », *Doc. Parl.,* Ch. Repr., sess. 1990-1991, 1610/1, p. 61.

[1707] Dans le même sens, voy. F. Kauff-Gazin, « Vers une conception européenne de l'indépendance des autorités de régulation ? », *Europe,* 2010, p. 15. Cette auteure affirme que « la nomination des membres de l'autorité par le gouvernement [...] peut poser problème au regard de l'indépendance effective et concrète des membres. Une fois nommés, il n'est pas sûr que les membres concernés s'affranchissent totalement d'une proximité ou d'une 'sensibilité' gouvernementale ».

sens, en tout cas, que se prononce la section de législation du Conseil d'État. Constatant qu' « un grand nombre de responsables des traitements sont des autorités publiques dépendant du pouvoir exécutif », elle soutient que « ce droit exclusif de présentation conféré au pouvoir exécutif et la logique majoritaire qui le sous-tend, ne sont pas en parfaite harmonie avec la nature des missions [de la Commission] »[1708]. Rappelons également que cette situation pose question au regard de la position de la Cour de justice de l'Union européenne, pour qui l'exigence d'indépendance impose que les membres de l'autorité de protection des données doivent exercer leur fonction en dehors de toute influence extérieure, qu'elle soit directe ou indirecte[1709]. Enfin, l'Agence des droits fondamentaux de l'Union européenne émet une crainte semblable. Elle cite la Belgique comme un des États dans lequel la procédure de désignation des membres de l'autorité de protection des données implique l'intervention de l'exécutif, du législatif et du judiciaire et ne manque pas de préciser que « it is essential to ensure that the Government does not, in practice, control directly or indirectly the majority of the appointees, thus effectively frustrating the purpose of a pluralistic nomination procedure »[1710].

Toutefois, il n'est pas évident de trouver une solution à ce problème. En effet, dans l'hypothèse où les candidats seraient présentés par la Chambre des représentants, on peut craindre que le problème demeure identique, compte tenu du fait qu'en définitive, les chefs de parti politique exercent probablement une grande influence sur le choix du candidat présenté. Nous reviendrons sur cette question dans le troisième chapitre[1711].

504.- La composition de la CPVP.

a) Le souci du pluralisme et de l'expertise. Comme on l'a déjà évoqué, la CPVP comprend en son sein la Commission et les comités sectoriels. La composition de ces organes est marquée par un pluralisme des intérêts représentés, et un souci d'expertise des membres. Ainsi, siègent au sein de la CPVP, au moins un juriste, au moins un magistrat, ainsi que plusieurs experts, à savoir, au moins un informaticien, un spécialiste de la

[1708] SLCE, avis du 2 février 1998 sur un avant-projet de loi « transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *Doc. Parl.,* Ch. Repr., sess. 1997-1998, n° 1566/1, p. 240.

[1709] Voy. *supra,* n° 497.-

[1710] European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* précité, pp. 19-20.

[1711] Voy. *infra,* n° 569.-

gestion des données dans le secteur public et un spécialiste de la gestion des données dans le secteur privé.

Quant aux comités sectoriels institués au sein de la CPVP, ils sont composés pour moitié de membres de la CPVP, et pour moitié de membres externes désignés en fonction de leur expertise[1712]. La désignation d'« assesseurs externes spécialisés » est présentée comme un « gage de compétence et d'efficacité »[1713], tandis que la présence des membres de la CPVP au sein de chaque comité sectoriel se justifie par le souci d'unifier les solutions avancées en matière de protection des données à caractère personnel.

b) Les difficultés. Rappelons que l'exigence d'indépendance telle qu'interprétée récemment par la Cour de justice de l'Union européenne signifie que les membres d'une autorité de protection des données doivent être en mesure de procéder à un examen objectif et impartial des traitements de données mis en place, de manière à trouver un juste équilibre entre la protection de la vie privée et les intérêts qui commandent un libre circulation des données[1714]. C'est pour cette raison qu'elle désapprouve, notamment, le fait que le membre administrateur de l'autorité de protection des données autrichienne soit un fonctionnaire fédéral soumis à un contrôle de tutelle dans l'exercice de ses fonctions et que le personnel mis à disposition de cette autorité soit composé de fonctionnaires.

En Belgique, la composition de la CPVP telle qu'organisée actuellement par la loi pose question au regard de l'objectivité et de l'impartialité de certains membres. En effet, la loi du 8 décembre 1992 n'empêche pas que le fonctionnaire d'une administration soumise au contrôle de la CPVP soit également membre de cette Commission. La loi encourage même cette situation, en exigeant la présence, au sein de la CPVP, d'un spécialiste de la gestion des données dans le secteur public et en prévoyant que le Conseil des ministres présente les candidats, ce qui peut favoriser les membres issus de l'administration, comme expliqué plus haut. Dans cette

[1712] Art. 31*bis*, §2, de la loi du 8 décembre 1992 et art. 3 de l'arrêté royal du 17 décembre 2003 précité. La composition du comité sectoriel de la sécurité sociale et de la santé fait exception à cette règle, conformément à l'art. 37 de la loi du 15 janvier 1990 précitée.

[1713] Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.*, n° 50-1940/001, p. 12.

[1714] C.J.U.E., gde ch., 9 novembre 2010, *République fédérale d'Allemagne c. Commission, op. cit.*, §§ 18 et s.

hypothèse, ledit membre est à la fois le contrôleur et le contrôlé, ce qui sème le doute sur son impartialité.

Ce problème est d'autant plus important que certaines personnes sont à la fois membre de la CPVP et membre d'un ou plusieurs comités sectoriels. Rappelons, en effet, que la loi du 8 décembre 1992 impose que la moitié des membres d'un comité sectoriel émanent de la CPVP. Le problème du « contrôleur contrôlé » s'étend alors à plusieurs organes[1715].

2. L'indépendance institutionnelle de la CPVP

505.- Le rattachement à la Chambre des représentants. L'indépendance institutionnelle de la CPVP s'apprécie au regard des ressources mises à sa disposition et de la possibilité d'adopter des décisions à l'abri d'ordres ou d'injonctions provenant de l'extérieur. Le souci de garantir l'indépendance institutionnelle de la CPVP est à l'origine d'une modification importante de son statut, intervenue par la loi du 26 février 2003 précitée. Ainsi, instituée dans un premier temps auprès du Ministre de la Justice, la CPVP fonctionne aujourd'hui sous l'égide de la Chambre des représentants[1716].

Il ressort des travaux préparatoires que, par là, le législateur a voulu faire de la CPVP un « organe collatéral de la Chambre des représentants », ce qui lui « paraît plus logique »[1717], bien qu'il reconnaisse qu'une telle « intégration [...] n'a, selon une étude de droit comparé, pas d'équivalent dans les pays voisins »[1718]. Un tel changement de statut est justifié par le

[1715] Pour autant que de besoin, rappelons que la Banque-Carrefour de la sécurité sociale est la plus grande plateforme d'échanges d'informations existant actuellement. Elle est régulièrement concernée par les avis de la CPVP. En outre, les données qui circulent par son intermédiaire au sein et en dehors du réseau de la sécurité sociale sont soumises aux décisions des comités sectoriels compétents. Comment, alors, ne pas être surpris de constater que l'Administrateur général de la Banque-Carrefour de la sécurité sociale est un membre effectif de la CPVP ? Comment ne pas l'être plus encore en constatant qu'il est aussi membre effectif du comité sectoriel du Registre national, tandis que l'administrateur général adjoint de cette même Banque-Carrefour en est un membre suppléant ? Tous deux sont également membres sans voix délibérative, du comité sectoriel de la sécurité sociale et de la santé, tant dans la section sécurité sociale que dans la section santé. En d'autres termes, les hauts dirigeants de la Banque-Carrefour de la sécurité sociale sont en mesure d'exercer un pouvoir d'influence lors des délibérations relatives à des avis et des décisions qui les concernent directement.

[1716] Voy. *supra,* n° 487.-

[1717] Rapport fait au nom de la Commission de la Justice par M. Tony Van Parys relatif à la proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.*, n° 50-1940/005, p. 4.

[1718] *Ibid.*, p. 21. Voy. D. De Bot, *op. cit.,* pp. 387-389.

fait que « les compétences de la Chambre des représentants en matière de contrôle politique et en matière budgétaire, et plus généralement la place que lui reconnaît la Constitution, justifient que ce soit auprès d'elle que soit désormais placée la Commission »[1719], cette dernière ayant une mission de « contrôle de l'administration »[1720]. Cela devrait, en outre, « inciter davantage le Parlement à demander l'avis de la Commission sur les textes en projet »[1721]. Par ailleurs, la Commission est placée sous l'égide de la Chambre des représentants et non du Sénat car « à l'exception du comité R, toutes les institutions que le législateur a estimé opportun d'instituer sous l'égide d'une assemblée parlementaire le sont auprès de la Chambre des représentants (Conseil supérieur de la Justice, comité P, et le Collège des médiateurs) »[1722].

Désormais, le budget de la CPVP est fixé par la Chambre des représentants, ainsi que les règles applicables à son secrétariat. Au-delà, la CPVP exerce sa mission de manière indépendante. En effet, la loi précise que les membres de la CPVP ne reçoivent d'instructions de personne dans l'exécution de leurs tâches. De plus, la Chambre des représentants ne dispose que du droit de voir communiquer le rapport d'activité de la CPVP, ainsi que son règlement d'ordre intérieur, sans toutefois pouvoir modifier ce dernier.

L'indépendance institutionnelle de la CPVP semble donc renforcée par ce rapprochement à l'égard de la Chambre des représentants, dans la mesure où aucun contrôle de tutelle ne peut orienter les agissements de l'autorité de protection des données.

C. Une autorité légitime ?

506.- Indépendance et légitimité. L'autorité légitime est entendue ici comme l'autorité valablement fondée à agir dans notre société démocratique, compte tenu notamment des contrôles auxquels elle est soumise. En l'occurrence, on s'interroge sur la légitimité de la CPVP car l'indépendance de cette autorité génère un certain malaise au regard de deux principes constitutionnels fondamentaux, à savoir la responsabilité politique

[1719] *Doc. parl.,* Ch. repr., sess. 2001-2002, n° 50-1940/001, p. 10.

[1720] Rapport fait au nom de la Commission de la Justice par M. Tony Van Parys relatif à la proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.,* n° 50-1940/005, p. 4.

[1721] *Ibid.*, pp. 4-5.

[1722] *Doc. parl.*, Ch. repr., sess. 2001-2002, n° 50-1940/001, p. 10.

de l'administration et le principe d'indisponibilité des attributions dévolues au pouvoir exécutif[1723].

Une autre question surgit de la directive 94/46 qui tout à la fois impose l'indépendance de l'autorité de protection des données mais exige également, en son article 28, §3, que cette autorité soit soumise à un contrôle juridictionnel.

Des solutions doivent être trouvées pour rendre la CPVP responsable de son action. Mais est-il envisageable d'organiser le contrôle politique et juridictionnel d'une autorité sans porter atteinte à son indépendance ? Les lignes qui suivent sont consacrées à cette importante question.

§1. Le contrôle politique de l'autorité indépendante

507.- La Constitution et le droit européen. Le statut de la CPVP est soumis à une tension fondamentale. D'une part, les articles 33 et 37 de la Constitution imposent de soumettre cette autorité à un contrôle politique. D'autre part, la directive 95/46 impose une exigence d'indépendance qui a été récemment interprétée de manière très rigoureuse par la Cour de justice de l'Union. Comment, alors, concilier le droit constitutionnel et le droit européen ?

1. L'autorité indépendante et la Constitution

508.- Les articles 37 et 101, alinéa 1er, de la Constitution. La réforme législative de 2003 a fait sortir la CPVP du giron du pouvoir exécutif pour renforcer son indépendance[1724], ce qui explique qu'aujourd'hui, la CPVP n'est soumise ni au contrôle hiérarchique d'un ministre, ni à un contrôle de tutelle. Cette autorité dispose pourtant de prérogatives importantes et, en particulier, d'un pouvoir de décision contraignant qu'elle exerce par l'intermédiaire des comités sectoriels chargés d'autoriser ou de refuser le transfert des données dans l'administration. En d'autres termes, bien qu'étant une autorité externe au Gouvernement, elle dispose d'une parcelle du pouvoir de mettre en œuvre les lois.

[1723] Voy. *infra,* n° 508.- et s.

[1724] Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.*, n° 50-1940/001.

Ce constat pose question au regard de deux principes constitutionnels fondamentaux, qui découlent des articles 37 et 101, alinéa 1er, de la Constitution.

Le premier est la *responsabilité politique* du ministre du fait de l'administration. Comme l'explique Michel Pâques, « en droit constitutionnel belge, le Gouvernement dans son ensemble, qu'il soit fédéral, régional ou communautaire, les ministres, individuellement, sont responsables devant le Parlement fédéral, le Parlement de la communauté ou de la région dont les membres peuvent interroger, critiquer les ministres, leur retirer la confiance et les contraindre à démissionner. Si le pouvoir échappe au Gouvernement ou à ses membres, comment assurer encore un véritable contrôle parlementaire sur les décisions prises ? »[1725]. Cette question concerne directement la CPVP. Etant une autorité indépendante, ses décisions ne sont pas assumées par un ministre. Comment pourraient-elles alors être soumises au contrôle parlementaire ?

Le second principe est celui de *l'indisponibilité des compétences*. En vertu de l'article 37 de la Constitution, le pouvoir exécutif appartient au Roi. Or, confier à la CPVP le pouvoir de prendre des décisions en matière de protection des données s'apparente à un dessaisissement d'une partie du pouvoir exécutif au profit d'une autorité qui n'en fait pas partie. Faut-il considérer alors que le pouvoir de décision de la CPVP est inconstitutionnel ?

509.- La solution de la section de législation du Conseil d'État. Dans un premier temps, la section de législation, se fondant sur le principe de l'indisponibilité des compétences, a estimé que l'attribution d'un pouvoir de décision à une autorité qui n'est pas soumise au contrôle hiérarchique du pouvoir exécutif est inconstitutionnelle[1726].

Depuis lors, la section de législation du Conseil d'État a assoupli son interprétation. Elle admet aujourd'hui qu'un pouvoir de décision soit

---

[1725] M. Pâques, « Décentralisation, régulation et contrôle démocratique. L'arrêt 130/2010 en question », *Liber amicorum Marc Boes,* Brugge, die Keure, 2011, p. 415. Sur le contrôle parlementaire des autorités indépendantes, voy. dans également D. Déom, *Le statut juridique des entreprises publiques,* Bruxelles, Story-Scientia, 1990, p. 227 ; M. Leroy, *Les règlements et leurs juges,* Bruxelles, Bruylant, 1987, p. 98 ; X. Delgrange, L. Detroux et H. Dumont, « La régulation en droit public », *in Élaborer la loi aujourd'hui, une mission impossible ?,* Bruxelles, Publication des Facultés universitaires Saint-Louis, 1999, p. 76.

[1726] Voy. not. avis L. 33.487/1/3 des 18 et 20 juin 2002 sur un avant-projet de loi portant des mesures en matières de soins de santé, *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50-2125/1, p. 525 (cet avant-projet de loi octroyait au Conseil général de l'Institut national d'assurance maladie-invalidité le pouvoir de fixer et de répartir le budget concerné). Pour d'autres avis allant dans le même sens, voy. R. Andersen, P. Nihoul et M. Joassart, « Le Conseil d'État. Chronique de jurisprudence 2002 », *R.B.D.C.,* 2004, pp. 84 et 85.

attribué « à une autorité administrative dont la direction n'est pas assumée directement par les titulaires constitutionnellement ou légalement désignés du pouvoir exécutif [si et seulement si] ceux-ci exercent sur l'organisme un contrôle suffisant pour pouvoir en assumer la responsabilité politique » devant une assemblée démocratiquement élue.[1727] Un tel contrôle de tutelle apparaît donc « comme une manière de concilier la nécessité d'une responsabilité politique traditionnelle devant le Parlement et l'attribution à une autorité externe d'une portion de pouvoir »[1728].

L'intensité du « contrôle suffisant » du pouvoir exécutif sur l'autorité indépendante s'apprécie par rapport à l'étendue des pouvoirs qui sont confiés à cette dernière. Ainsi, si l'autorité en question dispose d'un large pouvoir discrétionnaire qui implique des choix d'opportunité, l'autorité politiquement responsable doit pouvoir exercer un contrôle en opportunité sur ses décisions. À l'inverse, si l'autorité de régulation ne dispose que d'un faible pouvoir d'appréciation n'étant chargée que d'appliquer une réglementation précise, seul un contrôle de légalité des décisions doit pouvoir être exercé[1729].

510.- Une application : le contrôle du Comité d'habilitation pour le Registre national et les cartes d'identité. La section de législation du Conseil d'État a appliqué cette interprétation au « Comité d'habilitation pour le Registre national et les cartes d'identité »[1730].

La section de législation du Conseil d'État constate l'attribution d'un large pouvoir décisionnel à ce Comité.

[1727] Avis L. 33.865/4 du 13 novembre 2002 sur un avant-projet de décret sur la radiodiffusion, *Doc. CCF,* sess. 2002-2003, n° 357/1, cité par R. Andersen, P. Nihoul et M. Joassart, « Le Conseil d'État. Chronique de jurisprudence 2002 », *op. cit.,* p. 86. Voy. également les nombreuses études consacrées à cette question, not. R. Andersen, « Les autorités administratives indépendantes en droit belge », *Annuaire européen de droit administratif,* 2008, p. 28 ; D. Delvax, « Les contrôles administratifs pesant sur les autorités administratives indépendantes », *Rev. Dr. ULB,* 2008, pp. 112 et s. ; E. Slautsky, « Droit européen, Constitution et autorités administratives indépendantes. Commentaire des arrêts de la Cour constitutionnelle du 18 novembre 2010, n° 130/2010 et du Conseil d'État du 7 avril 2011, *Ville de Wavre,* n° 212.557 », *A.P.T.,* 2012, pp. 108 et 109.

[1728] M. Pâques, « Décentralisation, régulation et contrôle démocratique. L'arrêt 130/2010 en question », *op. cit.,* p. 416.

[1729] Avis L. 33.255/4 du 5 juin 2002 sur un avant-projet de loi relatif au statut du régulateur des secteurs des postes et des télécommunications belges, *Doc. Parl.,* Ch. Repr., sess. 2001-2002, n° 1937/1, p. 62 ; Avis L. 33.865/4 du 13 novembre 2002 sur un avant-projet de décret sur la radiodiffusion, *op. cit.,* p. 87.

[1730] Ce comité à depuis lors été renommé en « Comité sectoriel du Registre national », mais il n'y a pas eu de modification de son pouvoir d'autorisation.

> La section de législation du Conseil d'État affirme que « le projet entend conférer au Comité d'habilitation un pouvoir de décision quant à l'accès au Registre national qui impliquera, dans certains cas, l'exercice d'un large pouvoir d'appréciation, notamment dans l'appréciation tant du caractère d'intérêt général des tâches pour lesquelles l'accès au Registre national serait sollicité par des organismes publics ou privés de droit belge, que des informations pour lesquelles, au regard des principes de finalité et de proportionnalité, cet accès serait autorisé »[1731].

Or, il s'agit d'une autorité sur laquelle « le Gouvernement n'exerce directement aucun pouvoir d'injonction, d'annulation ou de réformation » si bien que ses « activités échappent au contrôle des autorités publiques »[1732], ce qui déroge aux « principes constitutionnels d'attribution des pouvoirs »[1733] mais également aux règles visant à assurer la protection de la vie privée des citoyens[1734].

> À ce sujet, la section de législation du Conseil d'État rappelle que « le principe du maintien de la responsabilité politique du pouvoir exécutif a été la règle consacrée jusqu'à ce jour par la loi du 8 août 1983 [organisant un registre national des personnes physiques], et que le souci d'assurer la protection de la vie privée des personnes physiques doit être d'autant plus minutieux que l'article 22, alinéa 1er, de la Constitution dispose que 'chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi[1735]' et que la loi du 8 décembre 1992 [...] consacre, en son article 4, le principe de la collecte des données pour des finalités déterminées et légitimes, compte tenu notamment des dispositions légales et réglementaires applicables[1736] ».[1737]

Dès lors, comme elle l'avait déjà affirmé à propos du CSA[1738], la section de législation réclame qu' « à tout le moins » les dispositions légales en projet « soient complétées afin de mieux circonscrire le pouvoir d'appréciation reconnu au Comité d'habilitation »[1739], de manière à ce que le

---

[1731] Avis L. 33.962/2 du 27 janvier 2003 relatif à un projet de loi modifiant la loi du 8 août 193 organisant un registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *Doc. Parl.,* Ch. Repr., sess. 2002-2003, n° 50-2226/003, p. 6.

[1732] *Idem.*

[1733] *Idem.*

[1734] *Idem.*

[1735] C'est nous qui soulignons.

[1736] C'est nous qui soulignons.

[1737] Avis L. 33.962/2 précité, p. 6.

[1738] *Idem.*

[1739] *Idem.*

pouvoir exécutif puisse garder sur l'autorité en question, le contrôle suffisant pour pouvoir en assumer la responsabilité politique. En outre, elle demande à l'auteur du projet de loi qu'il « indique de manière expresse dans l'exposé des motifs les raisons pour lesquelles il est nécessaire de déroger » aux principes et règles qui viennent d'être mentionnés.

Malheureusement, le législateur n'a pas suivi la section de législation du Conseil d'État, au motif que « le présent projet de loi reprend la formulation qui a été retenue dans le projet de loi portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création des guichets-entreprises agrées et portant diverses dispositions [...]. Le Gouvernement souhaite que le parallélisme soit maintenu entre les deux projets de loi. Par ailleurs, il insiste sur le fait que des garanties suffisantes sont prévues dans le projet de loi quant au respect de la vie privée »[1740]. La disposition problématique a été adoptée à 12 voix contre 2 abstentions.

2. L'autorité indépendante et le droit européen

511.- Un contrôle de tutelle interdit. Comme il en a été question précédemment[1741], la Cour de justice de l'Union européenne s'est prononcée à deux reprises sur la portée de l'exigence d'indépendance des autorités de contrôle imposée par l'article 28 de la directive 95/46[1742].

a) L'arrêt du 9 mars 2010. Le premier arrêt, rendu le 9 mars 2010, est l'aboutissement d'un recours intenté par la Commission européenne.

[1740] Rapport du 14 février 2003 fait au nom de la Commission de l'Intérieur, des affaires générales et de la fonction publique par Corinne De Permentier, à propos du projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *Doc. Parl.,* Ch. Repr., session 2002-2003, n° 50-2226/005, p. 14.

[1741] Voy. *supra,* n° 497.-

[1742] C.J.U.E., gde ch., 9 mars 2010, *République fédérale d'Allemagne c. Commission,* précité. Pour un commentaire de cet arrêt, voy. M. Aubert, E. Broussy et F. Donnat, « Chronique de jurisprudence communautaire », *A.J.D.A.,* 2010, pp. 938 et 939 ; H.R. Kranenborg, « Commentaar », *SEW,* 2010, pp. 421 à 423 ; E. Debaets, « Les autorités administratives indépendantes et le principe démocratique : recherches sur le concept d' 'indépendance' », Rapport présenté au VIIIème Congrès mondial de l'association internationale de droit constitutionnel, Mexico, 6-10 décembre 2010 disponible sur le site www.juridicas.unam.mx/wccl/ponencias/14/254.pdf ; European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* 7 mai 2010, p. 19, disponible sur le site www.fra.europa.eu ; O. De Schutter, « Les droits fondamentaux dans l'Union européenne », *J.D.E.,* 2011, pp. 113 et 114.

Celle-ci reproche à l'Allemagne de soumettre les autorités de contrôle instituées au sein des *Länder* allemands, à un contrôle de tutelle.

Pour défendre cette situation, l'Allemagne invoque des motifs constitutionnels comparables à l'argumentation de la section de législation du Conseil d'État qui vient d'être analysée. L'Allemagne argue du fait que le régime démocratique organisé par la Constitution allemande exige une « soumission de l'administration aux instructions du Gouvernement, responsable devant le Parlement ». C'est pourquoi, « les autorités de contrôle en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel disposant de certains pouvoirs d'intervention à l'égard de citoyens [...] en vertu de l'article 28, paragraphe 3, de la directive 95/46, un contrôle élargi de la légalité de leurs activités au moyen d'instruments de contrôle de la légalité ou du fond serait absolument nécessaire »[1743].

Néanmoins, pour la Cour de justice de l'Union européenne, l'indépendance imposée à l'autorité de protection des données par la directive 95/46 est incompatible avec l'exercice d'un contrôle de tutelle sur ladite autorité. La Cour reconnaît que, certes, la tutelle a pour but de contrôler la légalité de l'action de l'autorité indépendante car, en l'occurrence, le contrôle de tutelle consiste à influer sur les décisions, voire les annuler ou les remplacer, dans le but de « garantir une action des autorités de contrôle qui soit conforme aux disposition nationales et communautaires applicables »[1744]. « Elle n'a donc pas pour objectif de contraindre lesdites autorités à éventuellement poursuivre des objectifs politiques contraires à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et aux droits fondamentaux ».

C'est d'ailleurs en se fondant sur ce même constat que l'avocat général avait conclu que le contrôle de tutelle était compatible avec l'indépendance de l'autorité de protection des données[1745].

Toutefois, deux raisons expliquent la méfiance de la Cour à l'égard de ce contrôle.

Premièrement, il n'est pas certain que le Gouvernement exerce correctement le contrôle de tutelle lorsqu'il s'agit des règles de protection des données à caractère personnel. La Cour affirme sans ambages que des abus peuvent être commis lorsqu'il est nécessaire, pour le Gouvernement,

---

[1743] C.J.U.E., gde ch., 9 novembre 2010, *République fédérale d'Allemagne c. Commission, op. cit.*, § 40.

[1744] *Ibid.*, §33.

[1745] Conclusions de l'avocat général M. Jan Mazak présentées le 12 novembre 2009 dans l'affaire ayant donné lieu à l'arrêt de la Cour de justice de l'Union européenne du 3 mars 2010 précité, §35.

« voire simplement utile, d'accéder à des bases de données pour accomplir certains missions, notamment à des fins fiscales ou répressives »[1746].

Deuxièmement, quand bien même la tutelle serait toujours exercée à bon escient, sa seule existence porte atteinte à l'indépendance objective et subjective de l'autorité de protection des données.

Considérant que l'indépendance implique l'absence de toute influence extérieure, la Cour soutient que « le seul risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle suffit pour entraver l'exercice des missions de celles-ci »[1747]. Elle se départit ainsi des conclusions de l'avocat général, qui suggérait à la Cour de rejeter le recours intenté par la Commission, arguant du fait que cette dernière n'avait pas démontré que le contrôle de tutelle empêchait effectivement l'exercice indépendant des missions des autorités de contrôle allemandes.

Deux raisons soutiennent l'assertion de la Cour. La première tient à l'indépendance subjective de l'autorité. Ainsi, le risque d'influence politique pourrait provoquer une « obéissance anticipée »[1748] de la part des autorités de contrôle. La seconde tient à l'indépendance objective du contrôleur : « le rôle de gardiennes du droit à la vie privée qu'assument lesdites autorités exige que leurs décisions, et donc elles-mêmes, soient au-dessus de tout soupçon de partialité »[1749].

Par conséquent, par son arrêt du 9 mars 2010, la Cour de justice de l'Union européenne condamne l'Allemagne, pour avoir soumis ses autorités de contrôle nationales à la tutelle du Gouvernement.

b) L'arrêt du 16 octobre 2012. Dans son deuxième arrêt, rendu le 16 octobre 2012[1750], la Cour de justice de l'Union européenne confirme l'ampleur de l'exigence d'indépendance et l'applique à l'autorité de protection des données autrichienne (la « DSK »). La Cour estime que l'organisation et le statut de la DSK se heurtent à l'exigence d'indépendance telle qu'elle l'a interprétée dans son arrêt du 9 mars 2010. Pour la Cour, il existe, en effet, un risque important que la Chancellerie fédérale exerce une influence sur la DSK et ses membres et ce, à trois égards.

Tout d'abord, le membre administrateur de la DSK, chargé de gérer les affaires courantes de cette autorité, est un fonctionnaire fédéral, comme l'impose le règlement d'ordre intérieur de la DSK. Il existe donc « un lien

1746 *Ibid.*, §35.
1747 *Ibid.*, §36.
1748 *Idem.*
1749 *Idem.*
1750 C.J.U.E., gde ch., 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10.

de service entre [ce membre] et l'autorité fédérale, qui permet au supérieur hiérarchique dudit membre administration de contrôler les activités de ce dernier »[1751]. Or, « ce pouvoir de contrôle [est] susceptible d'entraver l'indépendance de la DSK dans l'exercice de ses missions »[1752] car « il n'est pas exclu que l'évaluation par le supérieur hiérarchique du membre administrateur de la DSK en vue de favoriser l'avancement dudit fonctionnaire puisse conduire à une forme d'obéissance anticipée' dans le chef de ce dernier »[1753]. De plus, en raison de ce lien, la DSK ne se trouverait pas « au-dessus de tout soupçon de partialité »[1754].

Ensuite, le bureau de la DSK est composé de fonctionnaires de la chancellerie fédérale, sur lesquels cette dernière exerce un contrôle de tutelle[1755]. Il existe donc un risque d'influence de la Chancellerie fédérale sur les décisions de la DSK. Et, « en tout état de cause, une telle imbrication organisationnelle entre la DSK et la Chancellerie fédérale empêche que la DSK soit au-dessus de tout soupçon de partialité et est donc incompatible avec l'exigence d'indépendance »[1756].

Enfin, la Cour critique le droit du chancelier fédéral « de s'informer à tout moment auprès du président et du membre administrateur de la DSK, de tous les aspects de la gestion de ladite autorité de contrôle »[1757]. En outre, ce droit est inconditionnel. La Cour estime qu'un tel droit à l'information « s'oppose à ce que la DSK puisse être considérée comme pouvant opérer, en toute circonstance, au-dessus de tout soupçon de partialité »[1758].

Il résulte donc de cet arrêt que non seulement, la Cour de justice de l'Union européenne s'oppose à l'existence d'un contrôle de tutelle sur l'autorité de protection des données, mais également à tout lien entre le Gouvernement et la DSK, qui empêcherait cette dernière d'être placée « au-dessus de tout soupçon de partialité » selon l'expression de la Cour. C'est donc une impartialité subjective mais également objective qui est requise de la part de l'autorité de protection des données.

512.- Un contrôle parlementaire autorisé. Bien qu'elle s'oppose au contrôle du Gouvernement sur l'autorité de protection des données, la

[1751] *Ibid.*, § 49.
[1752] *Ibid.*, § 50.
[1753] *Ibid.*, § 51.
[1754] *Idem.*
[1755] *Ibid.*, § 59.
[1756] *Ibid.*, § 61.
[1757] *Ibid.*, § 63.
[1758] *Ibid.*, § 65.

Cour reconnaît l'importance d'assurer le contrôle parlementaire des autorités indépendantes, afin de conférer une légitimité démocratique à ces autorités qui prennent des décisions importantes à l'égard des citoyens sans être démocratiquement élues.

Répondant à l'argument de l'Allemagne qui, rappelons-le, affirmait que le contrôle de tutelle était nécessaire au vu du régime démocratique organisé par la Constitution, la Cour affirme que le principe de démocratie « ne s'oppose pas à l'existence d'autorités publiques situées en dehors de l'administration hiérarchique classique et plus ou moins indépendantes du Gouvernement. L'existence et les conditions de fonctionnement de telles autorités relèvent, dans les États membres, de la loi ou même, dans certains États membres, de la Constitution et ces autorités sont soumises au respect de la loi, sous le contrôle des juridictions compétentes. De telles autorités administratives indépendantes, ainsi qu'il en existe d'ailleurs dans le système juridique allemand, ont souvent des fonctions régulatrices ou exercent des missions qui doivent être soustraites à l'influence politique, tout en restant soumises au respect de la loi, sous le contrôle des juridictions compétentes. Tel est précisément le cas des missions des autorités de contrôle en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel ». Et d'ajouter que « l'absence de toute influence parlementaire sur ces autorités ne saurait se concevoir »[1759].

Selon la Cour, le contrôle parlementaire de l'autorité indépendante peut s'exercer sans passer par la responsabilisation d'un ministre devant le Parlement.

La Cour émet plusieurs propositions. « D'une part, les personnes assumant la direction des autorités de contrôle peuvent être nommées par le Parlement ou le Gouvernement. D'autre part, le législateur peut définir les compétences desdites autorités »[1760].

De plus, « le législateur peut imposer aux autorités de contrôle l'obligation de rendre compte au parlement de leurs activités. Un rapprochement peut être opéré, à cet égard, avec l'article 28, paragraphe 5, de la directive 95/46, qui prévoit que chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité, qui sera publié »[1761].

Et de conclure que « compte tenu de ce qui précède, le fait de conférer un statut indépendant de l'administration générale aux autorités de

[1759] C.J.U.E., gde ch., 9 mars 2010, *République fédérale d'Allemagne c. Commission, op. cit.*, §43.
[1760] *Ibid.*, §44.
[1761] *Ibid.*, §45.

contrôle en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le secteur non public n'est pas en soi de nature à priver ces autorités de leur légitimité démocratique »[1762].

513.- Critiques. L'incompatibilité décrétée par la Cour de justice de l'Union européenne entre l'exigence d'indépendance et le contrôle du Gouvernement peut s'apparenter à un argument d'autorité[1763] qui crée, dans l'ordre juridique belge, des difficultés juridiques fondamentales.

Rappelons que pour la Cour de justice de l'Union européenne, un lien trop étroit entre l'autorité de protection des données et le Gouvernement porterait atteinte à l'indépendance subjective et objective de l'autorité de protection des données. Or, en quoi le rapprochement de l'autorité en question au Parlement plutôt qu'au Gouvernement endiguerait ce danger ? Au contraire, la suppression du contrôle de tutelle semble provoquer un recul dans l'objectivité et l'impartialité des décisions de l'autorité indépendante. En effet, dans l'hypothèse où l'autorité n'agirait pas de manière indépendante – qu'elle soit soumise aux pressions du Gouvernement ou de toute autre sphère d'influence – le fait qu'un contrôle de tutelle existe permet au Parlement de mettre en cause un ministre, voire l'ensemble du Gouvernement. Cette possibilité doit donc inciter le ministre en question à veiller, constamment et préventivement, à la légalité de l'action de l'autorité indépendante. Par contre, si le contrôle de tutelle est supprimé au profit de la seule obligation de rendre au Parlement un rapport d'activité de l'autorité indépendante, les illégalités commises par cette dernière ne seront révélées qu'à la condition qu'un parlementaire minutieux, patient et courageux, étudie ledit rapport, confronte son contenu aux exigences du régime juridique de la protection des données à caractère personnel et convainque le Parlement de prendre des mesures à l'égard de l'autorité indépendante.

Dès lors, la solution de la Cour de justice de l'Union européenne « conduit ici à affaiblir le contrôle démocratique sur le pouvoir discrétionnaire [de l'autorité indépendante] en n'exigeant plus aucune tutelle et à écarter un principe fondamental de notre organisation constitutionnelle »[1764].

[1762] *Ibid.*, §46.

[1763] En ce sens, M. PÂQUES, « Décentralisation, régulation et contrôle démocratique. L'arrêt 130/2010 en question », *op. cit.*, p. 424.

[1764] *Idem.*

3. Vers une conciliation du droit constitutionnel et du droit européen ?

514.- La tension entre le droit constitutionnel et le droit européen. En somme, pour être légitime, l'autorité de protection des données doit être soumise à un contrôle de tutelle, en vertu du droit constitutionnel tel qu'interprété par la section de législation du Conseil d'État. En revanche, la directive 95/46 interdit un tel contrôle au nom de l'indépendance de l'autorité de protection des données, comme l'a affirmé la Cour de justice de l'Union européenne.

Comment résoudre cette tension ? L'arrêt rendu par la Cour constitutionnelle, le 18 novembre 2010, au sujet de l'indépendance de la Commission de régulation de l'électricité et du gaz[1765] (CREG) offre des éléments de réponse intéressants.

515.- L'origine de l'arrêt de la Cour constitutionnelle n° 130/2010. À l'origine de l'arrêt de la Cour constitutionnelle se trouve une décision de la CREG imposant une amende administrative à la Ville de Wavre. Mécontente, cette dernière a intenté un recours en annulation contre la sanction de la CREG, et demandé au Conseil d'État de poser une question préjudicielle à la Cour constitutionnelle. Bien qu'elles concernent la CREG, la question préjudicielle posée, et la réponse donnée par la Cour, nourrissent les réflexions relatives au statut de la CPVP.

En effet, la CREG, comme la CPVP, est une autorité de régulation qui dispose d'un pouvoir de décision sans être soumise au contrôle de tutelle d'un ministre. Cette situation est au cœur de la question préjudicielle posée par le Conseil d'État.

Par souci de clarté des analyses qui suivent, soulignons d'ores et déjà qu'à l'époque où la Cour constitutionnelle s'est prononcée dans cet arrêt et jusqu'à l'adoption, le 8 janvier 2012[1766], d'une loi transposant la nouvelle directive européenne en matière d'énergie, la CREG était soumise à un certain contrôle du pouvoir exécutif. En effet, elle devait faire rapport annuellement au ministre compétent au sujet de l'exécution de ses

[1765] C.C., arrêt n° 130/2010 du 18 novembre 2010 relatif à la question préjudicielle concernant la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité, en particulier ses art. 23, §2, al. 2, 15°, et 31, posée par le Conseil d'État, B.2.

[1766] Loi du 8 janvier 2012 portant modifications de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité et de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations, *M.B.,* 11 janvier 2012, p. 909. Sur les faibles garanties d'indépendance de la CREG avant cette modification législative, voy. T. Hennen et N. Petit, *op. cit.,* pp. 536 et 537.

missions[1767]. Elle devait aussi faire approuver, par le Gouvernement, sa note de politique générale[1768]. Par ailleurs, le Gouvernement pouvait suspendre et faire modifier les décisions tarifaires de la CREG[1769]. Il revenait également au Roi, ou au ministre qui a l'énergie dans ses attributions, de fixer la rémunération des membres, ce qui est toujours d'actualité[1770].

Depuis la modification législative intervenue le 8 janvier 2012 qui renforce l'indépendance des régulateurs nationaux, nombre de prérogatives du pouvoir exécutif sur la CREG ont été allégées voire supprimées.

Etant donné que la CREG n'est pas soumise au contrôle de tutelle d'un ministre, le pouvoir exécutif n'est pas en mesure d'exercer sur cette autorité un « contrôle suffisant pour en assumer la responsabilité devant une assemblée démocratiquement élue », comme l'exige pourtant la section de législation du Conseil d'État[1771]. Partant de là, doit-on considérer que le pouvoir réglementaire de la CREG est inconstitutionnel ? C'est la question qui a été posée à la Cour constitutionnelle.

Plus précisément, il s'agissait de savoir s'il existe une discrimination entre les destinataires « d'une décision des autorités administratives dont la direction est assurée directement par le pouvoir exécutif » et les destinataires des décisions de la CREG qui, de par son indépendance, échappe « au contrôle du pouvoir exécutif et, par conséquent, à la possibilité d'assumer devant la Chambre des représentants la responsabilité politique des actes qu'elle pose »[1772] ? En d'autres termes, le statut de la CREG viole-t-il les articles 10 et 11 de la Constitution, pris isolément et combinés avec les articles 33 et 37 de la Constitution ?

516.- La réponse de la Cour constitutionnelle. L'arrêt de la Cour tente de concilier notre système constitutionnel, qui s'oppose à ce qu'une autorité dotée d'un pouvoir de décision agisse en dehors de tout contrôle, avec les directives européennes qui imposent l'indépendance des autorités nationales de régulation.

[1767] Art. 23, §3, de la loi du 29 avril 1999 précitée, avant sa modification le 8 janvier 2012.

[1768] Art. 25, §3, al. 3, de la loi du 29 avril 1999 précitée, avant sa modification le 8 janvier 2012.

[1769] Art. 29, *sexies,* art. 25, §3, al. 3, de la loi du 29 avril 1999 précitée, avant sa modification le 8 janvier 2012.

[1770] Art. 24, §2, de la loi du 29 avril 1999 précitée.

[1771] Au sujet du renforcement de l'indépendance de la CREG, voy. A.-S. Renson, « L'indépendance des autorités de régulation : la fin d'une controverse », *J.T.,* 2011, p. 349 ; M. Pâques, « Décentralisation, régulation et contrôle démocratique. L'arrêt 130/2010 en question », *op. cit.*, pp. 411 à 424.

[1772] C.C., arrêt n° 130/2010, *op. cit.,* B.5.

La Cour constate ainsi que la « large autonomie » dont dispose la CREG dans l'exercice de ses missions est voulue par le droit européen.

> Ainsi affirme-t-elle que « le fait que la CREG exerce ses missions avec un degré élevé d'autonomie découle [...] des exigences du droit de l'Union européenne, qui est progressivement devenu plus explicite en l'espèce »[1773]. De nombreux paragraphes suivent cette affirmation, qui reprennent les directives européennes imposant cette autonomie[1774]. La Cour fonde son affirmation notamment sur l'article 35 de la directive 2009/72/CE précitée qui prévoit que l'autorité de régulation doit être « juridiquement distincte et fonctionnellement indépendante de toute autre entité publique ou privée »[1775].

Cette autonomie « n'est pas compatible avec la soumission de cette autorité à un contrôle hiérarchique ou à une tutelle administrative »[1776].

Selon la Cour, l'absence de contrôle hiérarchique et de tutelle sur la CREG ne viole pas la Constitution. En particulier, le respect de l'article 37 de la Constitution est assuré car cette disposition « ne s'oppose pas [...] à ce que, dans une matière technique déterminée, le législateur confie des compétences exécutives spécifiques à une autorité administrative autonome qui reste, pour le surplus, soumise tant au contrôle juridictionnel qu'au contrôle parlementaire ». Et d'ajouter que « par ailleurs, dans le considérant 34 de la directive 2009/72/CE, il est dit que l'indépendance du régulateur de l'énergie 'n'empêche ni l'exercice d'un contrôle juridictionnel, ni l'exercice d'un contrôle parlementaire conformément au droit constitutionnel des États membres' »[1777]. On peut dès lors comprendre que, selon la Cour, le pouvoir réglementaire d'une autorité indépendante est compatible avec l'article 37 de la Constitution, si l'exercice de ce pouvoir décisionnel est encadré par un contrôle juridictionnel et un contrôle parlementaire. En d'autres termes, le contrôle juridictionnel et le contrôle parlementaire sont les conditions de constitutionnalité d'une autorité indépendante disposant d'un pouvoir réglementaire.

[1773] *Ibid.,* B. 8.2.

[1774] Voy. *Ibid.,* B.8.2.1. à B.8.3.3.

[1775] Voy. *Ibid.,* B. 8.3.1 à B. 8.3.3. Une auteure s'est d'ailleurs étonnée que la Cour fonde son raisonnement sur les exigences du « 'troisième paquet énergie' qui n'avait pas encore vu le jour au moment des faits ayant donné lieu à la question préjudicielle en cause » si bien que l'on peut légitimement se demander si la justification de la Cour constitue « une argumentation surabondante à celle tirée du droit constitutionnel belge ou une véritable condition à la constitutionnalité de la large autonomie de la CREG ». [voy. A.-S. Renson, *op. cit.,* p. 350].

[1776] C.C., arrêt n° 130/2010, *op. cit.,* B.4.

[1777] *Ibid.,* B.5.

Ainsi, la Cour constitutionnelle soutient qu'une autorité indépendante dotée d'un pouvoir de décision ne doit pas nécessairement être soumise à un contrôle de tutelle. Elle pose néanmoins deux conditions à cette liberté. D'une part, un contrôle juridictionnel doit être exercé sur l'autorité indépendante. Cette exigence est remplie si les actes de ladite autorité peuvent être contestés devant une juridiction.

> En l'espèce, selon la Cour, la CREG est soumise à un contrôle juridictionnel car « les actes administratifs de la CREG peuvent faire l'objet d'un recours juridictionnel » devant le Conseil d'État, « juridiction indépendante et impartiale »[1778].

D'autre part, un contrôle parlementaire doit exister, ce qui est le cas lorsque le Parlement définit les missions et le fonctionnement de l'autorité indépendante, approuve son budget et qu'un rapport d'activités annuel lui est communiqué.

> Selon la Cour constitutionnelle, les décisions de la CREG sont soumises à un contrôle parlementaire, puisqu'« en exécution et dans les limites du droit de l'Union européenne, le législateur est compétent pour régler les missions et le fonctionnement de la CREG. Il lui appartient aussi d'approuver son budget. La CREG doit transmettre annuellement au ministre un rapport portant notamment sur l'exécution de ses missions et le ministre communique ce rapport annuel aux Chambres législatives fédérales et aux Gouvernements de région (article 23, § 3, de la loi du 29 avril 1999 en cause) »[1779].

À nouveau, un parallélisme peut être fait avec l'arrêt de la Cour de justice de l'Union européenne relatif à l'indépendance de l'autorité de protection des données, dans lequel des critères semblables sont utilisés pour vérifier l'existence d'un contrôle parlementaire. Dans l'arrêt du 9 mars 2010 précité, la Cour de justice de l'Union européenne a mentionné le pouvoir du Parlement de nommer les membres de l'autorité indépendante et de définir ses compétences, ainsi que l'obligation pour l'autorité indépendante de transmettre au Parlement un rapport d'activité à intervalles réguliers.

Néanmoins, à la différence de la Cour de justice de l'Union européenne, la Cour constitutionnelle ne se contente pas de ces critères. Elle conditionne le contrôle parlementaire à la possibilité d'interpeller un ministre pour les actes posés par l'autorité indépendante. La Cour constitutionnelle semble ainsi vouloir trouver une solution qui respecte l'interdiction

[1778] *Ibid.,* B.6.4. Nous y revenons au point suivant consacré au contrôle juridictionnel de l'autorité indépendante.

[1779] *Ibid.,* B.7.

de tutelle imposée par le droit européen, et la responsabilité parlementaire du pouvoir exécutif imposée par le droit constitutionnel. En effet, la Cour constitutionnelle affirme que les « chambres législatives peuvent par ailleurs, en usant des moyens de contrôle dont elles disposent, appeler le ministre compétent ou le Gouvernement fédéral à se justifier. Il ressort de ce qui précède qu'il existe bien un contrôle parlementaire »[1780].

La condition de l'interpellation du ministre crée toutefois un malaise juridique. En effet, pourquoi interpeller un ministre s'il n'a pas de droit de regard sur l'action de l'autorité indépendante et que sa mission « se borne à transmettre un rapport ? »[1781]. Selon Michel Pâques, « la responsabilité du ministre a un sens quand il exerce la tutelle, car, alors, le reproche d'avoir ou de ne pas avoir cautionné les actes sous tutelle a une vraie consistance. Devenu débiteur d'un service de transmission de document, comment pourrait-il mal s'en acquitter ? De quelle épaisseur est ce contrôle résiduel ? »[1782].

Dès lors, bien qu'il tente au mieux de concilier le droit européen et le droit constitutionnel, l'arrêt de la Cour constitutionnelle ne résout pas entièrement la question de savoir comment soumettre à un contrôle politique une autorité qui échappe au contrôle de tutelle. La troisième partie de ce titre tentera de proposer quelques pistes de solutions.

§2. Le contrôle juridictionnel de l'autorité indépendante

517.- Un contrôle juridictionnel imposé par le droit européen et confirmé par la Cour constitutionnelle. La directive 95/46 impose que les décisions de l'autorité de protection des données puissent faire l'objet d'un recours juridictionnel.

> L'article 28, §3, de la directive 95/46 prévoit en effet que « les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel ».
>
> Dans le même sens, la proposition de règlement européen sur la protection des données dispose que « toute personne physique ou morale a le droit de former un recours juridictionnel contre les décision d'une autorité de contrôle qui la concernent ». La proposition de règlement va même plus loin en affirmant qu'un recours juridictionnel peut également être formé contre

[1780] *Ibid.*, B. 7.

[1781] M. Pâques, « Décentralisation, régulation et contrôle démocratique. L'arrêt 130/2010 en question », *op. cit.*, p. 423. Dans le même sens, A.-S. Renson, *op. cit.*, p. 350 ; E. Slautsky, *op. cit.*, p. 111.

[1782] M. Pâques, « Décentralisation, régulation et contrôle démocratique. L'arrêt 130/2010 en question », *op. cit.*, p. 423.

> l'autorité de contrôle qui manquerait de réagir à la réclamation d'un citoyen. Ainsi, « toute personne concernée a le droit de former un recours juridictionnel en vue d'obliger l'autorité de contrôle à donner suite à une réclamation en l'absence d'une décision nécessaire pour protéger ses droits ou lorsque l'autorité de contrôle n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de sa réclamation [...] »[1783].

Par ailleurs, dans son arrêt n° 130/2010 précité, la Cour constitutionnelle a affirmé que le contrôle juridictionnel de l'autorité indépendante est une condition de sa constitutionnalité en vertu de l'article 37 de la Constitution[1784]. La possibilité d'attaquer les décisions de l'autorité indépendante devant la section du contentieux administratif du Conseil d'État remplit l'exigence d'un contrôle juridictionnel.

> Ainsi, selon la Cour, la CREG est soumise à un contrôle juridictionnel car « les actes administratifs de la CREG peuvent faire l'objet d'un recours juridictionnel » devant le Conseil d'État, « juridiction indépendante et impartiale »[1785], qui « procède à une contrôle juridictionnel approfondi, tant au regard de la loi qu'au regard des principes généraux du droit. Le Conseil d'État examine à cet égard si la décision de l'autorité soumise à son contrôle est fondée en fait, si elle procède de qualifications juridiques correctes et si la mesure n'est pas manifestement disproportionnée au fait établi. Lorsqu'il annule cette dernière, l'autorité est tenue de se conformer à l'arrêt du Conseil d'État : si l'autorité prend une nouvelle décision, elle ne peut méconnaître les motifs de l'arrêt annulant la première décision ; si elle s'en tient à l'annulation, l'acte attaqué est réputé ne pas avoir existé »[1786]. En outre, le Conseil d'État peut également « ordonner la suspension de l'exécution de la décision qui a imposé des sanctions, le cas échéant, en statuant en extrême urgence »[1787].

518.- La question de l'autorité administrative. Aucun recours juridictionnel n'est spécifiquement organisé pour contester les décisions de la CPVP[1788]. Il y a donc lieu de se demander si ces décisions sont attaquables

---

[1783] Art. 74 de la proposition de règlement européen sur la protection des données à caractère personnel.

[1784] C.C., arrêt n° 130/2010, *op. cit.,* B.5.

[1785] *Ibid.,* B.6.4.

[1786] *Ibid.,* B.6.2.

[1787] *Ibid.*, B.6.3.

[1788] En cela, la CPVP se distingue de la CREG, par exemple. En effet, les décisions de la CREG peuvent être attaquées par la voie d'un recours spécifique organisé devant la Cour d'appel de Bruxelles siégeant comme en référé (art. 29*bis* de la loi du 29 avril 1999 précitée. À ce sujet, voy. X. Taton, *Les recours juridictionnels en matière de régulation. Energie, communications électroniques, audiovisuel, transports, finance et concurrence,* Bruxelles, Larcier, 2010 ; P. Boucquey et P.-O. de Broux, *op. cit.,* pp. 256 et 257).

devant la section du contentieux administratif du Conseil d'État[1789]. Cela suppose que soit reconnue à la CPVP la qualité d'autorité administrative au sens de l'article 14 des lois coordonnées sur le Conseil d'État, puisque seules les décisions de ces autorités sont attaquables devant cette juridiction.

Remarquons que la loi sur la motivation formelle des actes administratifs[1790] et la législation fédérale sur la transparence administrative[1791] ne s'appliquent également qu'aux autorités administratives. Or, ces lois présentent un lien étroit avec le contrôle juridictionnel des actes contestés devant le Conseil d'État. En effet, si l'acte attaqué n'est pas motivé, comment en examiner la légalité[1792] ? Par ailleurs, la publicité des documents ayant servi de base à la décision administrative est bien souvent nécessaire également pour comprendre cette dernière. Ainsi, en reconnaissant la qualité d'autorité administrative à la CPVP, le contrôle juridictionnel de ses décisions serait garanti.

Malgré son importance en droit administratif, la notion d'autorité administrative ne fait l'objet d'aucune définition légale. S'interprétant au regard de la jurisprudence du Conseil d'État, de la Cour constitutionnelle et de la Cour de cassation, elle constitue une notion évolutive. Néanmoins, plusieurs critères sont traditionnellement utilisés par le Conseil d'État pour vérifier si l'acte soumis à sa censure émane d'une autorité administrative. On distingue, parmi ceux-ci, les critères négatifs et les critères positifs[1793].

[1789] À la différence des décisions de la CREG, pour lesquelles un recours spécifique est organisé devant la Cour d'appel de Bruxelles siégeant comme en référé, aucun recours n'est spécifiquement organisé pour contester les décisions de la CPVP. La section du contentieux administratif du Conseil d'État est donc la seule juridiction à propos de laquelle il y a lieu de se demander si elle pourrait juger la légalité d'une telle décision.

[1790] Loi du 29 juillet 1991 sur la motivation formelle des actes administratifs. Voy. *supra,* n° 313.- et s.

[1791] Loi du 11 avril 1994 relative à la publicité de l'administration. Voy. *supra,* n° 252.- et s.

[1792] À ce sujet, voy. C.C., arrêt n° 17/2004 du 29 janvier 2004 relatif à la question préjudicielle concernant la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs, posée par le Conseil d'État. La Cour y affirme que « l'absence d'obligation de motivation formelle ne permettrait pas au Conseil d'État d'exercer un contrôle efficace » (B.6.2).

[1793] Parmi les nombreuses contributions doctrinales traitant des critères de l'autorité administrative, voy. not. A. Rasson-Roland, « Note d'observation »., *A.P.T.,* 1982, p. 79 ; G. Boland, « La notion d'autorité administrative », *A.P.T.,* 1988, p. 81 ; W. Lambrechts, « De evolutie van het begrip administratieve overheid », *T.B.P.,* 1987, pp. 357-366 ; R. Andersen, « L'obligation de motiver : pour quelles autorités administratives ? », *in La motivation formelle des actes administratifs. Loi du 29 juillet 1991. Actes de la journée d'étude du 8 mai 1992,* Brugge, La Charte, 1992, p. 61 ; D. Delvax, « Flux et reflux de la jurisprudence relative à la notion d'autorité administrative », *A.P.T.,* 2001, p. 196 ; P. Nihoul, « La notion d'autorité administrative : retour à l'orthodoxie », *A.P.T.,* 2001, pp. 204 et 205 ; D. De Roy, « Etre

Par application des critères négatifs, les institutions qui relèvent du pouvoir législatif ou du pouvoir judiciaire ne sont pas des autorités administratives.

Les critères positifs qui retiennent l'attention sont, d'une part, la création ou l'agrémentation de l'institution par ou en vertu d'un texte de valeur législative et l'existence d'un contrôle des pouvoirs publics sur le fonctionnement et la gestion de cette institution. Ces critères sont dits « organiques ». D'autre part, l'exercice, par cette institution, d'une mission d'intérêt général et le pouvoir de l'institution de prendre unilatéralement des décisions contraignantes à l'égard des tiers constituent des critères « fonctionnels ». Ces critères positifs ne sont pas nécessairement appliqués de manière cumulative, ce qui complexifie l'exercice d'identification de l'autorité administrative. Une institution peut ainsi être considérée comme une autorité administrative alors même que certains des critères mentionnés ne seraient pas remplis.

> Par exemple, la société SOFICO est une autorité administrative car elle est créée par décret sous la forme d'une personne morale de droit public, elle exerce une mission d'intérêt général, et ses activités sont soumises au contrôle de la Région et ce, même si elle ne dispose pas du pouvoir de prendre des décisions contraignantes à l'égard des tiers[1794].

Compte tenu des critères négatifs et positifs de l'autorité administrative, la question de savoir si la CPVP est une autorité administrative doit se résoudre en deux temps. Dans un premier temps, il convient de vérifier si la CPVP relève du pouvoir législatif ou du pouvoir judiciaire, auquel cas cette institution doit d'emblée être exclue de la notion d'autorité

---

ou ne pas être … autorité administrative. Vers de nouvelles questions existentielles pour les A.S.B.L. satellites des institutions communales ? », *Dr. Comm.,* 2002, p. 202 ; D. Deom, « Enseignement libre et autorité administrative : dis-moi oui, dis-moi non », *A.P.T.,* 2004, p. 100 ; D. De Roy, « Le pouvoir réglementaire des autorités administratives indépendantes en droit belge », *in Rapports belges au Congrès de l'Académie internationale de droit comparé à Utrecht* (dir. E. Dirix et Y.-H. Leleux), Bruxelles, Bruylant, 2006, n° 11 et 12 ; F. Vandendriessche, *Publieke en private rechtspersonen,* Brugge, die Keure, 2004, pp. 252-276 ; A.-L. Durviaux, « La notion d'autorité administrative en débats », note sous C.E. n° 176.478 du 6 novembre 2007, *C.D.P.K.,* 2008, pp. 854 et 855 ; C. Baekeland, « De VZM als 'Administratieve overheid' in de zin van art. 14, §1, 1° RVS – Wet : De Weg van de verwekking tot de geboorte », *C.D.P.K.,* 2010, pp. 455 à 465 ; M. Leroy, *Contentieux administratif,* 5e éd., Limal, Anthemis, 2011, pp. 265 à 286.

[1794] C.E., *Algemene Aannemingen Van Laere,* n° 176.478, du 6 novembre 2007, pp. 11 à 13. Cet arrêt concerne un recours en annulation contre la décision de la SOFICO d'attribuer un marché public. Au sujet de cet arrêt, voy. A.-L. Durviaux, « La notion d'autorité administrative en débats », note sous C.E. n° 176.478 du 6 novembre 2007, *op. cit.,* pp. 854 à 858.

administrative. Dans la négative, la CPVP doit être confrontée aux critères positifs de l'autorité administrative.

1. La CPVP au regard des critères négatifs de l'autorité administrative

519.- Un organe du pouvoir judiciaire ? Dans l'exercice de sa compétence de gestion des plaintes[1795], la CPVP présente des caractéristiques qui se rapprochent de celles d'une juridiction administrative. Différents indices sont utilisés pour identifier une juridiction administrative[1796]. On est ainsi attentif à la nature de l'acte juridictionnel, qui tranche un conflit entre des prétentions contradictoires et est assorti d'une motivation, et à l'opération intellectuelle effectuée par le juge, qui consiste à confronter les faits aux règles de droit pour en dégager une solution juridique. Le fondement juridique d'une juridiction importe également. Celle-ci doit être instituée par le législateur. Un autre indice tient au statut indépendant de la juridiction et à la contradiction des débats. Enfin, on sera attentif à l'autorité de la chose jugée de la décision juridictionnelle, qui explique que cette dernière ne peut être contestée que par les voies de recours que la loi organise et ne peut plus être remise en cause par la suite.

La question se pose de savoir si la CPVP doit effectivement être considérée comme une juridiction, auquel cas, la réponse donnée à une plainte doit pouvoir être attaquée devant la section du contentieux administratif du Conseil d'État dans le cadre d'un recours en cassation[1797].

Il ressort de l'article 31 de la loi du 8 décembre 1992 et des articles 25 et suivants du règlement d'ordre intérieur de la CPVP[1798] que certains indices tenant à la *nature de l'acte* permettraient de qualifier la décision de la CPVP d'acte juridictionnel. En effet, en réponse à une plainte portée auprès d'elle, la CPVP tranche un litige qui lui a été soumis, en le confrontant aux règles de droit applicable. En outre, sa décision doit être motivée[1799].

[1795] Les indices d'une juridiction administrative ne sont pas présents dans le cadre des autres missions de la CPVP. En effet, dans l'exercice de sa compétence d'avis, la CPVP ne tranche pas de litige ni ne rend de décision. Quant aux décisions rendues par les comités sectoriels institués au sein de la CPVP, elles ne concernent pas un litige à proprement parler, ne sont pas soumises à une exigence de motivation ni de contradictoire.

[1796] Sur ces caractéristiques, voy. not. M. Leroy, *Contentieux administratif, op. cit.,* pp. 103 à 109.

[1797] Art. 20 des Lois coordonnées sur le Conseil d'État.

[1798] Ce règlement d'ordre intérieur est disponible à l'adresse suivante : http://www.privacycommission.be/sites/privacycommission/files/documents/05.01.02.02-reglement_ordre_interieur_cpvp.pdf

[1799] Art. 31, §4, de la loi du 8 décembre 1992.

Par ailleurs, certains indices tiennent au *statut et à l'organisation* de la CPVP qui est soumise à des exigences d'indépendance et d'impartialité. Ainsi, le président et les membres ne peuvent recevoir d'instructions de personne et ne peuvent être relevés de leur charge en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent pour remplir leurs fonctions[1800]. Il est également interdit aux membres de la CPVP d'être présents lors de la délibération sur les objets pour lesquels ils ont un intérêt personnel ou pour lesquels leurs parents ou alliés jusqu'au quatrième degré ont un intérêt personnel[1801]. En outre, la CPVP doit comprendre au moins un magistrat[1802]. Des règles de procédure doivent aussi être respectées, puisque le principe du contradictoire doit être respecté lors de l'instruction des plaintes[1803].

Malgré la présence de tels indices, le pouvoir de « décision » de la CPVP n'est pas assimilable au pouvoir de décision d'un juge. C'est ce que le Conseil d'État, section du contentieux administratif, a décidé suite à un recours en cassation porté devant lui.

> Cette affaire concerne un litige survenu en 2008 entre Anne-Marie Lizin et la CPVP. À l'origine, un conseiller communal de Huy décide, en 2007, d'interroger par courrier la CPVP sur la légalité de certains traitements de données effectués alors dans la commune de Huy, dont le Bourgmestre est Anne-Marie Lizin. Celle-ci envoie depuis de nombreuses années une carte de prompt rétablissement aux personnes hospitalisées au CHR de Huy, ce qui suppose la réutilisation des données détenues par le CHR. En outre, le Collège des Bourgmestre et Echevins organise un grand nombre d'inaugurations dans certains quartiers rénovés, en invitant nominativement les personnes habitant les quartiers en question, à partir d'une sélection de ces citoyens dans le registre des électeurs. Enfin, les autorités communales identifient les étrangers non européens pour les inviter à certaines rencontres en vue de répondre à leurs questions sur le droit de vote.
>
> En réponse au courrier qui lui a été adressé par le conseiller communal de Huy, la CPVP fait état de l'illégalité de la plupart de ces pratiques, au motif qu'elles violent le principe de finalité auquel sont soumis les traitements de données à caractère personnel ainsi que la protection applicable aux données dites « sensibles » car, en l'occurrence, les données ont trait à l'état de santé et à l'origine raciale.
>
> Recevant cette réponse, le conseiller communal concerné alerte la presse qui diffuse cette information. Faisant état du fait qu'elle n'a pas pu faire

[1800] Art. 24, §4 et §6 de la loi du 8 décembre 1992.

[1801] Art. 24, §7, de la loi du 8 décembre 1992.

[1802] Art. 24, §1, de la loi du 8 décembre 1992.

[1803] Art. 31, §2, de la loi du 8 décembre 1992 et art. 31 du règlement d'ordre intérieur précité.

> valoir son point de vue devant la CPVP, Anne-Marie Lizin intente un recours en cassation contre la « décision » de la CPVP.
>
> Par une ordonnance du 21 mai 2008[1804], le Conseil d'État, section du contentieux administratif, juge que « le recours en cassation est manifestement irrecevable » car « l'acte contre lequel le recours est formé n'est pas une décision d'une juridiction administrative ». Le Conseil d'État justifie ce constat en soutenant que « si la loi porte bien que [les] 'décisions' [de la CPVP] sont motivées, elle ne lui confère aucun pouvoir de décision ; que l'indépendance que le législateur a assuré à la Commission par des dispositions similaires à certains éléments du statut des magistrats, pas plus que le caractère contradictoire de la procédure à suivre n'ont pour effet de conférer à la Commission vie privée un caractère juridictionnel »[1805].

Bien que l'on puisse regretter que la décision du Conseil d'État ne soit pas plus amplement motivée, on en approuve le contenu. Le raisonnement du Conseil d'État se fonde sur l'analyse de l'article 31 de la loi du 8 décembre 1992.

> L'article 31 de la loi du 8 décembre 1992 est formulé comme suit : « §1er. Sans préjudice de toute action devant les tribunaux et sauf si la loi en dispose autrement, la Commission examine les plaintes signées et datées qui lui sont adressées. Ces plaintes peuvent avoir trait à sa mission de protection de la vie privée, à l'égard des traitements de données à caractère personnel ou à d'autres missions qui lui sont confiées par la loi.
>
> § 2. La procédure est réglée par le règlement d'ordre intérieur. Celui-ci prévoit l'exercice d'un droit de défense.
>
> § 3. La Commission examine la recevabilité de la plainte. Si la plainte est recevable, la Commission accomplit toute mission de médiation qu'elle juge utile. En cas de conciliation des parties, fondée sur le respect de la vie privée, elle dresse un procès-verbal dans lequel la solution retenue est explicitée. En l'absence de conciliation, la Commission émet un avis sur le caractère fondé de la plainte. Son avis peut être accompagné de recommandations à l'intention du responsable du traitement.
>
> § 4. Les décisions, avis et recommandations de la Commission sont motivés.
>
> § 5. La Commission communique sa décision, son avis ou ses recommandations au plaignant, au responsable du traitement et à toutes les autres parties à la cause. Une copie de la décision, de l'avis ou des recommandations est adressée au Ministre de la Justice ».

[1804] C.E., 21 mai 2008, *Vandersteepen,* n° 2724.

[1805] *Ibid.,* p. 4.

Cette disposition met en évidence la volonté du législateur d'assurer un caractère non conflictuel à la procédure de plainte. En effet, la médiation est privilégiée pour concilier les parties. Si la conciliation n'est pas possible, la CPVP « émet un avis sur le caractère fondé de la plainte », qui peut être accompagné de « recommandations à l'intention du responsable du traitement ». Il est dès lors étonnant de voir apparaître soudainement le terme « décision » dans les paragraphes 4 et 5, sans comprendre lors de quelle phase de la procédure de plainte intervient la « décision ». Il eut été moins maladroit de ne viser que les avis et les recommandations de manière à ne pas douter du caractère non juridictionnel de l'acte rendu par la CPVP.

520.- Un organe de la Chambre des représentants ? Rappelons que la loi du 26 février 2003 a « institué auprès de la Chambre des représentants une Commission de la protection de la vie privée, composée de membres désignés par la Chambre des représentants, parmi lesquels le président et le vice-président »[1806]. La CPVP doit-elle pour autant être qualifiée d'organe collatéral de la Chambre des représentants ? La question mérite d'être abordée avec prudence. En effet, si la CPVP est un organe collatéral de la Chambre, elle ne peut être qualifiée d'autorité administrative. Les conséquences d'un tel constat seraient importantes. Dans cette hypothèse, les décisions de la CPVP ne pourraient pas être attaquées au Conseil d'État et la CPVP ne serait pas tenue de respecter les obligations de transparence consacrées par la loi du 11 avril 1994 sur la publicité de l'administration et la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs.

La qualité d'organe de la Chambre des représentants est attribuée aux autorités qui sont instituées auprès de la Chambre et sont également liées à celle-ci de façon suffisamment étroite[1807]. Pour juger de l'existence de ce lien suffisamment étroit, le Conseil d'État est attentif à plusieurs critères.

Il s'agit tout d'abord de la *composition* de l'institution. Le Conseil d'État vérifie le rôle que joue la Chambre dans la composition de l'autorité en question.

> Par exemple, le Collège des médiateurs fédéraux est un organe collatéral de la Chambre des représentants[1808]. Les deux médiateurs fédéraux sont nommés

[1806] Art. 23 de la loi du 8 décembre 1992.

[1807] R. Andersen, *op. cit.*, p. 60 ; A. Rasson-Roland, *op. cit.*, p. 81.

[1808] La section de législation du Conseil d'État affirme que le médiateur fédéral est une « autorité quasi parlementaire qui exerce des activités collatérales à celles de la Chambre des représentants ». Voy. SLCE, avis du 8 décembre 1993 sur un avant-projet de loi « instaurant un médiateur », *Doc. Parl.*, Ch. repr., session 1993-1994, n° 48-1436/1, p. 15.

par la Chambre des représentants, qui peut les révoquer dans des hypothèses limitées[1809]. Leur statut et leurs responsabilités sont fixés par la loi[1810].

La Cour des comptes est aussi qualifiée d'organe collatéral de la Chambre des représentants par le Conseil d'État[1811]. La Chambre des représentants nomme les membres de la Cour des comptes. C'est elle aussi qui fixe le barème de leur traitement[1812].

Le *mode de fonctionnement* de l'autorité est également un critère pour identifier un organe collatéral de la Chambre. Il s'agit d'identifier si la Chambre intervient dans la fixation et l'octroi du budget de l'institution, et dans la définition de son règlement d'ordre intérieur. La question de savoir si l'organe doit rendre compte de son activité – notamment par le biais de la remise de rapports réguliers – a également son importance.

Reprenons les exemples du Collège des médiateurs fédéraux et de la Cour des comptes, tous deux considérés comme des organes collatéraux de la Chambre.

Le règlement d'ordre intérieur du Collège des médiateurs fédéraux doit être approuvé par la Chambre des représentants[1813]. Celui de la Cour des comptes ne peut être modifié qu'avec l'accord de la Chambre[1814].

Par ailleurs, les médiateurs fédéraux et les membres de la Cour des comptes doivent rendre compte annuellement à la Chambre des représentants[1815].

Enfin, la *mission* accomplie par l'autorité en question est examinée. En particulier, pour être qualifiée d'organe collatéral de la Chambre, les tâches imparties à l'institution en question doivent contribuer suffisamment aux missions dévolues à la Chambre.

Les médiateurs fédéraux exercent un contrôle administratif externe[1816], raison pour laquelle ils ne peuvent contrôler que les autorités administratives

---

[1809] L'art. 6 de la loi du 22 mars 1995 prévoit que les médiateurs ne peuvent être révoqués que s'ils exercent un mandat incompatible avec la fonction de médiateur et proscrit par la loi du 22 mars 1995, ainsi que pour des motifs graves.

[1810] Il s'agit de la loi du 22 mars 1995 instaurant des médiateurs fédéraux, *M.B.,* 7 avril 1995.

[1811] C.E., 6 février 1952, *De Vos,* n° 1292, *Rec.*, pp. 86-87 ; C.E., 18 mai 1953, *Casteleyn,* n° 2469, pp. 650-651 ; C.E., 29 octobre 1953, *Manouvrier,* n° 2870, pp. 1222-1225 ; C.E., 19 novembre 1954, *Bette,* n° 3823, p. 978 ; C.E., 23 février 1978, *Trine,* n° 18781, pp. 222-224. Voy. Ch. HUBERLANT, *op. cit.*, pp. 65 à 68.

[1812] Art. 1er de la loi du 29 octobre 1846 relative à l'organisation de la Cour des comptes.

[1813] Art. 17 de la loi du 22 mars 1995 instaurant des médiateurs fédéraux.

[1814] Art. 20 de la loi du 29 octobre 1846 relative à l'organisation de la Cour des comptes.

[1815] Art. 15 de la loi du 22 mars 1995 instaurant des médiateurs fédéraux ; art. 8 de la loi du 29 octobre 1846 relative à l'organisation de la Cour des comptes.

[1816] H. WUYTS, « De ombudsman in perspectief », *T.B.P.,* 1999, pp. 416-417.

au sens de l'article 14 des lois coordonnées sur le Conseil d'État[1817]. De cette manière, les médiateurs fédéraux contribuent à la fonction de contrôle du pouvoir exécutif exercée par la Chambre des représentants.

La Cour des comptes participe à la fonction de contrôle financier dont la Chambre des représentants a la charge. De manière générale, elle dénonce à la Chambre tout manquement aux lois budgétaires[1818]. En cela, sa tâche est liée étroitement à celle de la Chambre[1819].

A contrario, le Conseil supérieur de la justice n'est pas qualifié d'organe collatéral de la Chambre. Bien que « la moitié de ses membres [soit] choisie par le Sénat » et qu'il soit « fait rapport tous les ans, notamment à la Chambre des représentants et au Sénat, sur le fonctionnement général du pouvoir judiciaire »[1820], cela ne peut suffire à établir un lien suffisant avec le pouvoir législatif. Une attention particulière doit, en effet, être portée à la mission dont il a la charge. Or, le Conseil supérieur de la justice ne participe pas à suffisance à la fonction législative. En effet, cette autorité « n'intervient pas [...] dans le processus de confection de la loi, même si, comme d'autres autorités publiques, il peut faire des suggestions, et même rédiger des propositions, aux fins d'améliorer la législation dans le domaine de la justice. Le Conseil n'est pas non plus investi de mission de contrôle politique à l'encontre des membres du Gouvernement ou des services administratifs »[1821].

En l'occurrence, nous doutons que la CPVP soit un organe collatéral de la Chambre des représentants. Nos hésitations émanent du constat qu'avant 2003, la CPVP était qualifiée d' « autorité administrative indépendante » par la section de législation du Conseil d'État[1822]. Depuis lors, la loi du 26 février 2003 n'a pas modifié substantiellement l'organisation de la CPVP. Certes, la CPVP n'est plus instituée auprès du Ministère de la justice. Elle a quitté le giron du pouvoir exécutif afin de gagner davantage d'indépendance institutionnelle, administrative et financière[1823], ce qui

---

[1817] Art. 1, 3°, de la loi du 22 mars 1995 précitée.

[1818] Art. 14 de la loi du 29 octobre 1846 sur la Cour des comptes.

[1819] Art. 180 de la Constitution ; loi du 29 octobre 1846 relative à l'organisation de la Cour des comptes. Voy. F. Delpérée, *Le droit constitutionnel de la Belgique,* Bruxelles, Bruylant, Paris, L.G.D.J., 2000, pp. 722-723 ; M. Uyttendaele, *Précis de droit constitutionnel belge,* 3e éd., Bruxelles, Bruylant, 2005, pp. 732-733.

[1820] F. Delpérée, « Le statut et la composition du Conseil supérieur de la justice », *in Le Conseil supérieur de la justice* (dir.M. Verdussen), Bruxelles, Bruylant, 1999, p. 37.

[1821] *Idem*. Dans le même sens : D. de Bruyn, « Le Conseil supérieur de la justice », *J.T.,* 1999, p. 2.

[1822] Voy. *infra,* n° 577.-

[1823] Voy. not. Rapport fait au nom de la Commission de la Justice par M. Tony VAN PARYS relatif à la proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour

répond aux exigences européennes[1824]. Cette modification soulève des questions quant à la qualité d'autorité administrative de la CPVP[1825] mais ne fait pas nécessairement de la CPVP un organe collatéral de la Chambre. En effet, ni la composition de la CPVP, ni son mode de fonctionnement et encore moins ses missions n'ont été modifiées par la loi du 26 février 2003. On se demande donc s'il existe réellement un lien suffisamment étroit entre la CPVP et la Chambre.

C'est principalement l'apparente lâcheté du lien entre les *missions* de la CPVP et celles de la Chambre des représentants qui explique notre scepticisme[1826]. En effet, contrairement au Collège des médiateurs fédéraux et à la Cour des comptes, la CPVP n'a pas été créée pour aider la Chambre dans l'exercice du contrôle politique du Gouvernement. En outre, elle ne participe que partiellement à la fonction de législation. Cela se manifeste dans la définition des compétences de la CPVP.

Ainsi, s'agissant de la fonction de législation, la CPVP peut certes, par ses avis et ses recommandations, aider les Chambres législatives dans la rédaction des textes de lois en jouant le rôle « d'experts chargés de leur dire dans quels cas il est possible de déroger à la protection constitutionnelle de la vie privée et dans quelle mesure »[1827]. Toutefois, cette aide n'est pas réservée exclusivement à la Chambre des représentants ni même, plus largement, à la fonction législative[1828]. Si la CPVP s'est vu dotée, dès son origine, d'une telle compétence, c'est bien parce qu'elle a été voulue comme « un organe de la conscience sociale, sorte d'ombudsman ou de 'chien de garde' »[1829] dans la protection des données à caractère personnel, afin de garantir au citoyen que le traitement de celles-ci « et les

---

de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.,* n° 50-1940/005, p. 5. Voy. aussi le plan de gestion de la CPVP, disponible sur www.privacycommission.be

[1824] Voy. *supra,* n° 493.- et s.

[1825] Voy. *infra,* n° 575.- et s.

[1826] Dans le même sens, voy. le rapport du 17 décembre 2010 de l'Auditeur R. WIMMER à propos du recours en annulation introduit par Madame A.-M. Lizin contre une décision de la CPVP. Cette affaire a été détaillée plus haut. Voy. *supra,* n° 479.-

[1827] Rapport fait au nom de la Commission de la Justice par M. Tony VAN PARYS relatif à la proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *op. cit.,* n° 50-1940/005.

[1828] La CPVP peut en effet donner son avis soit d'initiative, soit sur demande des Chambres législatives mais aussi du Gouvernement, des Exécutifs communautaires et régionaux, des Conseils de communauté et régionaux, du Collège réuni ou de l'Assemblée réunie de la COCOF, COCOM ou COCON.

[1829] Y. POULLET, « Les autorités de contrôle : 'vues' de Bruxelles », *op. cit.,* p. 72.

échanges de données qui l'accompagnent sont effectués avec le souci de respecter et de protéger ses droits en matière de vie privée »[1830]. Il est d'ailleurs étonnant de constater que la CPVP fut d'abord placée sous l'égide du Ministre de la Justice de manière presque naturelle. Elle fut ensuite placée auprès de la Chambre, sans que sa compétence consultative n'ait été modifiée. En définitive, si un tel changement fut possible, ne serait-ce pas parce que la mission de la CPVP n'est liée spécifiquement ni à celle du Ministre de la Justice, ni à celle de la Chambre des représentants ?

D'autre part, la CPVP participe tout aussi partiellement à la mission de contrôle du Gouvernement. Les comités sectoriels sont compétents pour autoriser la communication de données à caractère personnel. Ces informations sont détenues par différents services publics fédéraux.

> Ainsi, le Service public fédéral Économie détient-il le registre « Banque-Carrefour des entreprises »[1831], tandis que le Service public fédéral Intérieur est en possession du registre national des personnes physiques[1832] et le Service public fédéral Justice, de la banque de données « Phénix »[1833]. Les données sociales sont, quant à elles, détenues par un organisme public institué auprès du Service public fédéral Sécurité sociale[1834].

En ce que les comités sectoriels peuvent empêcher ces services publics fédéraux de délivrer certaines données qu'ils détiennent, il semble permis de considérer qu'ils exercent un certain contrôle sur l'action du Gouvernement, ou, du moins, des quelques services publics fédéraux concernés. Ces derniers ne sont toutefois pas les seuls visés par le contrôle des comités sectoriels. En effet, le Gouvernement n'est pas seul demandeur d'accès aux données. Pour ne prendre qu'un exemple parmi d'autres, l'autorisation d'accès à des données du registre national peut être octroyée aux notaires et aux huissiers et justice, notamment[1835]. Ces personnes là sont donc, elles aussi, soumises au contrôle de la CPVP. La collaboration avec la Chambre des représentants n'est donc pas la mission première des comités sectoriels. Ceux-ci ont, avant toute autre chose, été créés pour filtrer l'accès aux données personnelles des citoyens et contribuer par là à une protection plus effective de la vie privée. Le contrôle des quelques services publics fédéraux concernés, et, par là, l'aide apportée à la Chambre des représentants, n'est donc qu'une conséquence de cet objectif premier

[1830] CPVP, Plan de gestion, p. 3, disponible sur www.privacycommission.be

[1831] Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises.

[1832] Loi du 8 août 1983 organisant un registre national des personnes physiques.

[1833] Loi du 10 août 2005 instituant le système d'information Phenix.

[1834] Il s'agit de la Banque-Carrefour de la sécurité sociale. Voy. la loi du 15 janvier 1990 relative à l'institution d'une Banque-Carrefour de la sécurité sociale.

[1835] Voy. art. 5 de la loi précitée du 8 août 1983.

mais n'en est pas l'incarnation. On ne peut donc pas raisonnablement en conclure que la CPVP aurait été instituée pour aider la Chambre dans son contrôle de l'action gouvernementale.

La composition et le mode de fonctionnement de la CPVP ne sont guère plus convaincants pour reconnaître à cette institution la qualité d'organe collatéral de la Chambre.

L'analyse de la *composition de la CPVP* éclaire difficilement nos réflexions sur la qualification de cette institution. En effet, un lien entre la Chambre et la CPVP se marque au niveau du pouvoir de la Chambre de nommer les membres de la CPVP, ces derniers ne pouvant toutefois faire partie d'une des assemblées législatives. Toutefois, ce constat n'est pas fort utile, car aussi bien la Cour des comptes – considérée comme un organe collatéral du Parlement – que le Conseil supérieur de la justice – auquel une telle qualité a été déniée – sont composés de membres désignés par une assemblée législative sans en faire partie. Par ailleurs, la Chambre des représentants peut relever les membres de leurs charges, mais ce pouvoir est strictement subordonné à la condition que la personne visée ait commis de graves manquements à sa fonction, contrairement à son pouvoir concernant les membres de la Cour des comptes. Ceux-ci peuvent, en effet, être révoqués par la Chambre des représentants, que la personne concernée ait commis une faute disciplinaire ou ait perdu la confiance de la Chambre[1836].

Quant au *mode de fonctionnement de la CPVP,* la Chambre des représentants est chargée de fixer le budget de la CPVP sur proposition de cette dernière[1837]. C'est elle aussi qui détermine les règles applicables au personnel du secrétariat de la CPVP[1838]. Pour le reste, la Chambre ne dispose que du droit de se voir communiquer le règlement d'ordre intérieur de la CPVP[1839] et son rapport d'activité[1840]. Par ailleurs, la loi précise que les membres de la CPVP ne reçoivent d'instructions de personne dans l'exécution de leurs tâches[1841]. À nouveau, il serait audacieux de vouloir trouver dans ces éléments des indices décisifs de l'existence d'un organe collatéral de la Chambre des représentants. Bien que cette dernière ait un certain pouvoir concernant le budget et le secrétariat de la CPVP, celle-ci semble assez indépendante dans l'exercice de sa mission. Elle dispose de

[1836] Art. 1, al. 3, de la loi du 29 octobre 1846 relative à l'organisation de la Cour des comptes.
[1837] Art. 34 de la loi.
[1838] Art. 35 de la loi.
[1839] Art. 28 de la loi.
[1840] Art. 32, §2, de la loi.
[1841] Art. 24, §6, de la loi.

son propre secrétariat. De plus, certains frais, tels que les frais de fonctionnement du comité sectoriel de la sécurité sociale, ne sont pas pris en charge par la Chambre[1842]. Par ailleurs, l'établissement de son règlement d'ordre intérieur ne requiert pas l'accord de l'assemblée législative, à la différence du Collège des médiateurs fédéraux. Enfin, bien que la Chambre doive être informée du rapport d'activité de la CPVP, ses membres ne reçoivent aucune instruction et les comités sectoriels décident souverainement d'octroyer ou non les autorisations sollicitées.

En conclusion, la confrontation des caractéristiques de la CPVP aux indices traditionnellement appliqués par le Conseil d'État sème un sérieux doute sur le fait que la CPVP serait un organe collatéral de la Chambre des représentants. Compte tenu du fait que la CPVP ne répond pas pleinement aux critères négatifs qui viennent d'être étudiés, on ne peut pas exclure que la CPVP est une autorité administrative. Qualifier la CPVP d'autorité administrative contribuerait d'ailleurs à assurer une meilleure protection des droits des citoyens, comme l'expliquent les développements qui suivent.

2. La CPVP au regard des critères positifs de l'autorité administrative

521.- La confrontation de la CPVP aux critères positifs de l'autorité administrative. La CPVP est-elle une autorité administrative ? Ainsi qu'on l'a déjà dit[1843], cette question est importante. Dénier à la CPVP la qualité d'autorité administrative reviendrait à empêcher que ses décisions puissent être soumises à la censure du Conseil d'État et que les obligations de transparence lui soient imposées.

L'étude du statut de la CPVP suppose qu'on confronte cette dernière aux critères positifs de l'autorité administrative parmi lesquels, rappelons-le[1844], on distingue les critères fonctionnels et les critères organiques.

La CPVP répond aux critères *fonctionnels* de l'autorité administrative. En effet, la CPVP exécute une mission d'intérêt général, celle de protéger la vie privée des citoyens dans les actes impliquant la communication de données à caractère personnel. En outre, elle dispose du pouvoir de prendre unilatéralement des décisions contraignantes à l'égard des tiers, ce pouvoir étant exercé par l'intermédiaire des comités sectoriels institués en son sein.

[1842] Art. 43, de la loi du 15 janvier 1990 précitée.
[1843] Voy. *supra,* n° 520.-
[1844] Voy. *supra,* n° 518.-

Quant aux critères *organiques*, la CPVP répond de toute évidence au critère de la création de l'institution par ou en vertu d'un texte de valeur législative puisque la CPVP est instituée par les articles 23 et suivants de la loi du 8 décembre 1992.

Par contre, le critère du contrôle de l'institution par les pouvoirs publics se vérifie moins volontiers dans le chef de la CPVP. L'appréciation de ce critère est délicate en l'espèce. D'un côté, plusieurs éléments font douter de la réalité d'un tel contrôle. Ainsi, les membres de la CPVP ne sont pas nommés par un ministre, bien qu'ils soient présentés par le Conseil des ministres[1845]. Ils ne peuvent pas non plus faire partie d'un département ministériel[1846]. Ils ne reçoivent pas d'ordre d'un ministre, puisqu'ils ne peuvent recevoir d'instructions de personne[1847]. La CPVP n'est pas non plus contrôlée par le pouvoir exécutif dans l'accomplissement de sa mission. Enfin, aucun ministre n'est responsable des décisions prise par cette autorité. D'un autre côté, certains indices attestent quand même d'une certaine influence des pouvoirs publics sur la CPVP. Premièrement, lorsqu'une demande d'autorisation d'accès à des données parvient à la CPVP, cette dernière la communique au comité sectoriel concerné mais aussi à l'institution de gestion du secteur concerné[1848]. Concrètement, ces institutions de gestion se confondent avec des organes du pouvoir exécutif puisqu'il s'agit du Service public fédéral Economie, du Service public fédéral Intérieur, de la Banque-Carrefour de la sécurité sociale ou du Service public fédéral des Technologies de l'information et des communications, selon le type de données visé par la demande d'accès[1849]. Une fois l'avis transmis, l'institution de gestion est invitée à donner un avis technique et juridique au comité sectoriel compétent. Si le comité ne rend pas de décision endéans un certain délai après réception de l'avis, celle-ci est réputée conforme à l'avis de l'institution de gestion[1850]. Deuxièmement, certains frais de fonctionnement du comité sectoriel pour la sécurité sociale sont pris en charge par la Banque-Carrefour de la sécurité sociale, et non par la dotation confiée par la Chambre des représentants à la CPVP[1851]. Troisièmement, la loi autorise les comités sectoriels à s'établir

[1845] Art. 24, §4, de la loi du 8 décembre 1992.

[1846] Art. 5, §1, de l'arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP.

[1847] Art. 24, §6, de la loi du 8 décembre 1992.

[1848] Art. 31*bis*, §3, de la loi du 8 décembre 1992.

[1849] Arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP ; art. 42 de la loi du 15 janvier 1990 précitée.

[1850] Art. 31*bis*, de la loi du 8 décembre 1992.

[1851] Art. 42 de la loi du 15 janvier 1990.

au siège de l'institution de gestion qui les concerne, plutôt qu'au siège de la CPVP[1852].

En conséquence, l'on peut affirmer que la CPVP n'est pas soumise à un réel contrôle des pouvoirs publics. Elle est toutefois influencée par le pouvoir exécutif puisque l'institution de gestion, organe du pouvoir exécutif, peut donner un avis aux comités sectoriels et que l'exécutif peut apporter une aide matérielle à certains comités.

522.- L'importance de soumettre la CPVP aux obligations imposées aux autorités administratives. Les développements qui précèdent montrent que la CPVP répond à la majorité des critères de l'autorité administrative. Néanmoins, le critère de la soumission de la CPVP au contrôle des pouvoirs publics se vérifie de manière moins évidente[1853]. Pour l'heure, il n'est donc pas certain qu'on puisse considérer que la CPVP est une autorité administrative.

À notre sens, une solution doit toutefois être trouvée pour soumettre cette institution aux obligations qui s'imposent aux autorités administratives. La CPVP plaide d'ailleurs elle-même en ce sens, affirmant qu' « il est primordial, en vertu de la directive, que le comité de surveillance[1854] jouisse d'une totale indépendance, que la publication des autorisations soit assurée et que celles-ci puissent faire l'objet d'un recours »[1855].

Cette solution pourrait émaner du Conseil d'État qui reconnaîtrait à la CPVP la qualité d'autorité administrative, ou du législateur qui modifierait l'article 14 des Lois coordonnées sur le Conseil d'État pour soumettre la CPVP au régime juridique applicable aux autorités administratives. Ces pistes de réflexion sont expliquées dans le troisième chapitre[1856].

La nécessité de soumettre la CPVP aux obligations imposées aux autorités administratives se justifie au regard de la directive 95/46. Cette solution est également nécessaire pour garantir le respect de plusieurs droits fondamentaux consacrés par la Constitution, à savoir, le droit à l'égalité et à la non discrimination, le droit à la protection de la vie privée et le droit à la transparence administrative.

[1852] Art. 31*bis,* §5, de la loi du 8 décembre 1992.

[1853] Ce constat s'explique par la grande exigence d'indépendance qui s'impose à la CPVP, et qui est étudiée de manière détaillée dans la suite de cette recherche. Voy. *infra*, n° 567.- et s.

[1854] En l'occurrence, il s'agit du comité de surveillance pour les données relatives aux véhicules, qui était organisé par un projet de loi, à l'image des comités sectoriels.

[1855] CPVP, avis n° 42/2006 du 18 octobre 2006 concernant l'avant-projet de loi portant création d'une source authentique des données relatives aux véhicules, n° 45.

[1856] Voy. *infra,* n° 575.- et s.

a) La justification au regard de l'article 28, §3, de la directive 95/46. L'article 28, §3, de la directive 95/46 concerne directement l'organisation de recours juridiques contre les décisions rendues par la CPVP. Cette disposition affirme, en effet, que « les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel ».

Le caractère inconditionnel de cette obligation impose d'organiser, dans l'ordre juridique belge, un recours juridictionnel contre les décisions de la CPVP. Reconnaître à la CPVP la qualité d'autorité administrative est une solution qui répond à cet impératif puisque, ce faisant, le Conseil d'État peut connaître des recours intentés contre les décisions de la CPVP.

L'obligation d'organiser un recours juridictionnel contre les décisions de l'autorité de protection des données se comprend d'ailleurs aisément au regard de la volonté des instances européennes d'organiser, dans les États membres, un contrôle fiable et efficace des traitements de données à caractère personnel, considéré comme un « élément essentiel de la protection des personnes à l'égard des traitements de données à caractère personnel »[1857].

> La proposition de règlement européen sur la protection des données confirme la nécessité de soumettre l'autorité de protection des données à un contrôle juridictionnel. Elle renforce même ce contrôle. En effet, l'article 74, intitulé « droit à un recours juridictionnel contre une autorité de contrôle », affirme que toute personne doit non seulement pouvoir former un recours juridictionnel contre les décisions de ladite autorité, mais il faut également lui permettre de former un tel recours pour obliger l'autorité de protection des données à donner suite aux réclamations qui lui sont adressées.

b) La justification au regard des articles 10 et 11 de la Constitution. L'article 31*bis* de la loi du 8 décembre 1992[1858] octroie une prérogative d'autorité administrative à la CPVP, à savoir, un pouvoir de décision unilatéral et contraignant à l'égard des tiers. S'il fallait considérer que la CPVP n'est pas soumise au régime juridique applicable aux autorités administratives, la Cour constitutionnelle pourrait considérer que l'article 31*bis* de la loi du 8 décembre 1992 est contraire aux articles 10 et 11 de la Constitution, pris isolément et combinés avec les articles 33 et 37 de la Constitution. En effet, contrairement aux destinataires des décisions des autorités administratives, les destinataires des décisions de la CPVP ne peuvent pas intenter de recours juridictionnel contre ces décisions.

[1857] Considérant 62 de la Directive 95/46.

[1858] Cette disposition prévoit notamment que « la loi institue au sein de la Commission des comités sectoriels compétents pour instruire et statuer sur des demandes relatives au traitement ou à la communication de données [...] ».

Pourtant, on perçoit difficilement en quoi une telle discrimination serait fondée sur une justification raisonnable. En effet, les citoyens doivent bénéficier de la même protection juridique à l'égard des décisions de même nature et ce, peu importe qu'elles émanent d'une autorité instituée au sein du pouvoir exécutif ou non. C'est ce qu'affirme la Cour constitutionnelle qui soutient que « la nature juridique [de l'institution auteure de la décision] n'a toutefois aucune incidence sur les [décisions rendues par cette institution] et sur les recours qui permettent d'en contester la légalité »[1859].

> Dans cet arrêt de la Cour constitutionnelle, il était question d'un recours d'un étudiant de l'ULB à l'égard d'une décision d'une commission chargée de délivrer des attestations pour les études de science dentaire et instituée au sein de l'ULB. Cette décision n'était pas attaquable devant le Conseil d'État car le pouvoir organisateur de l'ULB est un établissement de droit privé, ce qui empêche que l'on qualifie l'ULB d'autorité administrative, à la différence d'une université officielle dont le pouvoir organisateur est un établissement de droit public. La Cour constitutionnelle a jugé cette situation contraire aux articles 10 et 11 de la Constitution[1860].

Les articles 10 et 11 de la Constitution s'opposent également à ce que la CPVP ne soit pas soumise aux obligations de transparence applicables aux autorités administrative. La position de la CADA à ce sujet le confirme. Considérant que la CPVP n'est pas une autorité administrative[1861], la CADA affirme qu'elle n'est pas compétente pour se prononcer sur le refus du Comité sectoriel de la sécurité sociale et de la santé de divulguer des documents qu'il détient. La CADA déplore cette situation, arguant du fait que « l'absence de toute protection juridique doit être considérée comme étant contraire aux articles 10 et 11 de la Constitution lorsque le Comité sectoriel de la sécurité sociale et de la santé prend une décision sur l'octroi d'autorisations »[1862].

c) La justification au regard de l'article 22 de la Constitution. Le droit à la protection de la vie privée s'entend aujourd'hui du droit à l'autodétermination informationnelle, comme nous l'avons expliqué précédemment[1863]. En d'autres termes, chaque citoyen a le droit de garder la maîtrise de ses données bien que l'environnement numérique encourage la circulation opaque de ses informations. À cet égard, nous avons montré

[1859] C.C., arrêt n° 41/2003 du 9 avril 2003 concernant la question préjudicielle relative à l'article 14 des lois coordonnées sur le Conseil d'État, posée par le Conseil d'État, B.6.

[1860] *Ibid.*, B.6 et B.8.

[1861] Voy. *supra*, n° 290.-

[1862] CADA, avis n° 2011-309 précité, p. 9.

[1863] Voy. *supra*, n° 64.-

combien les législations organisant la transparence de l'administration, la motivation formelle des actes administratifs et les recours au Conseil d'État contre les décisions administratives sont autant de moyens d'action permettant au citoyen de garder une certaine maîtrise de ses données.

Partant de là, il importe d'appliquer ces législations à toute autorité impliquée dans le traitement de données des citoyens. La CPVP est la première institution visée par cette préoccupation. D'une part, elle détient nombre de documents qui permettraient aux personnes intéressées de comprendre la structure de l'e-gouvernement et les outils mis à sa disposition. La CPVP détient également des documents d'étude favorisant la compréhension du régime juridique de la protection des données. D'autre part, la CPVP rend des décisions intéressant directement les citoyens soucieux de comprendre la circulation de leurs données. On pense surtout aux décisions des comités sectoriels qui autorisent les échanges de données entre les administrations. Ces décisions doivent pouvoir être contestées sous peine de priver la protection des données d'une effectivité réelle.

En définitive, il est piquant de se remémorer que le souci de protéger au mieux la vie privée des citoyens est à la base de la réforme du statut de la CPVP par la loi du 26 février 2003. On souhaitait, par cette modification, renforcer la fiabilité et l'efficacité du travail de la CPVP, chargée, rappelons-le pour autant que de besoin, de veiller à la protection de la vie privée de chacun. Il est dès lors paradoxal de constater que cette modification pourrait conduire aujourd'hui à diminuer le contrôle des citoyens sur leurs données en faisant de la CPVP non pas un allié, mais un organisme étrange, voire étranger, entouré de secret et de remparts contre la contestation.

d) La justification au regard de l'article 32 de la Constitution. Concernant plus particulièrement le secret qui entoure actuellement les documents détenus par la CPVP, nous avons affirmé dans le Titre II de la recherche qu'il serait contraire au droit fondamental à la transparence administrative, consacré par l'article 32 de la Constitution, de ne pas soumettre la CPVP aux obligations de transparence traditionnellement appliquées aux autorités administratives en vertu de la loi du 11 avril 1994 sur la publicité de l'administration[1864]. C'est d'ailleurs la raison pour laquelle la constitutionnalité de la loi du 11 avril 1994 sur la publicité de l'administration peut être contestée, en ce qu'elle limite les obligations de transparence aux autorités administratives[1865]. En effet, les travaux préparatoires de l'article 32 de la Constitution font état du fait que le constituant

[1864] Voy. *supra,* n° 291.-
[1865] Voy. *supra,* n° 290.-

a entendu donner à ce droit fondamental une interprétation « aussi large que possible »[1866].

> Rappelons, en guise d'exemple, qu'il a été affirmé, à une seule reprise, qu' « on peut notamment renvoyer à l'article 14 des lois sur le Conseil d'État et la jurisprudence du Conseil d'État à ce sujet »[1867].
>
> Rappelons également que la CADA abonde dans le même sens. Elle a encore affirmé récemment que « le [constituant] visait [...] un domaine d'application personnel très vaste, mais a laissé au législateur le soin de l'interpréter. Vu le fait qu'il s'agit d'un droit fondamental, le législateur doit opter pour un contenu aussi vaste que possible. Par ailleurs, lorsque pour l'interprétation du champ d'application personnel le législateur opte pour la notion 'd'autorité administrative', il ne peut pas interpréter cette notion de manière si restrictive que la loi serait en contradiction avec le champ d'application que le [constituant] envisageait »[1868].

Dès lors, une solution doit être envisagée afin d'organiser la publicité des documents détenus par la CPVP, comme on l'explique dans le troisième chapitre.

II. Les moyens d'action de la CPVP

523.- Le contrôle des traitements de données en projet, en cours et contestés. Depuis sa création, la CPVP dispose de moyens de contrôle s'exerçant sur les traitements de données en projet et les traitements de données faisant l'objet de contestations. Depuis la loi du 26 février 2003, elle s'est vu attribuer également un pouvoir de décision concernant les traitements de données en cours. Par ailleurs, la CPVP accomplit une mission d'information et d'assistance en matière de protection des données à caractère personnel.

La CPVP se prononce sur les traitements de données en projet. Elle dispose, en effet, d'une compétence d'*avis* au sujet des normes applicables aux traitements de données à caractère personnel[1869].

[1866] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Note explicative, *Doc. Parl.*, Ch. repr., session 1992-1993, n° 839/1, p. 5.

[1867] *Idem*. C'est nous qui soulignons.

[1868] CADA, avis n° 2011-309, du 10 octobre 2011, sur le refus de donner accès à des documents qui ont été utilisés par le Comité sectoriel de la sécurité sociale et de la santé pour prendre une décision.

[1869] Art. 29 de la loi du 8 décembre 1992.

La CPVP est également attentive aux traitements de données en cours. Elle peut adresser des *recommandations,* qui visent des problématiques générales[1870] ou sont adressées à un responsable de traitement en particulier. Les indications fournies par cette voie sont non contraignantes.

Par ailleurs, comme on l'a déjà souligné, l'intégration des comités sectoriels au sein de la CPVP a abouti à conférer à cette dernière un réel pouvoir de *décision*[1871]. Ce pouvoir consiste à octroyer ou refuser l'autorisation de communiquer des données à caractère personnel enregistrées dans des sources authentiques. Ces autorisations émanent du comité sectoriel compétent pour le secteur concerné et ont pour objet la vérification de la légalité des traitements de données concrètement effectués.

Enfin, la CPVP dispose également du pouvoir d'intervenir lorsqu'un traitement de données à caractère personnel est contesté, en dénonçant le traitement au Procureur du Roi ou en initiant une procédure judiciaire. Le plus souvent, la contestation du traitement émane d'un citoyen qui dépose plainte[1872].

A. Le contrôle des traitements de données en projet : les avis

524.- Considérations générales. Avant qu'ils soient organisés par une norme et rendus effectifs, les traitements de données en projet sont soumis à l'examen de la CPVP. Celle-ci rend alors un avis dont le contenu et la portée sont analysés dans cette partie.

§1. Le contenu de l'avis

525.- Article 29 de la loi du 8 décembre 1992. En vertu de l'article 29, §1er, de la loi du 8 décembre 1992, la CPVP émet des avis « sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de [la loi du 8 décembre 1992] ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel ».

[1870] On pense, par exemple, aux recommandations relatives aux intégrateurs de service dans le secteur public (recommandation n° 03/2009) ou aux sources authentiques de données (recommandation n° 09/2012), par lesquelles la CPVP propose la définition de ces concepts-clé pour l'e-gouvernement, et indique une méthode à suivre pour utiliser ces outils conformément aux exigences de la protection des données à caractère personnel.

[1871] Art. 31*bis* de la loi du 8 décembre 1992.

[1872] CPVP, rapport d'activité 2010, *op. cit.*, p. 12.

Bon nombre d'avis de la CPVP concernent des normes en projet. C'est particulièrement le cas pour les avis rendus en matière d'e-gouvernement, dont il est question dans cette section.

La CPVP peut également exercer sa compétence d'avis quant à l'application du régime de la protection des données à des cas particuliers, suite à une question posée ou une plainte déposée[1873].

La compétence d'avis de la CPVP est générale puisque cette autorité est susceptible d'examiner tous les traitements de données à caractère personnel au regard des principes de la protection de la vie privée et des données à caractère personnel, que ceux-ci soient organisés par la loi du 8 décembre 1992 ou toute autre loi particulière. L'ampleur de cette tâche constitue donc une charge de travail importante et ce d'autant plus que la matière à traiter est telle qu'elle impose aux membres de la CPVP de prendre connaissance des technologies en constante évolution, et, bien souvent, d'en comprendre la technicité. Cette tâche peut d'ailleurs aboutir à une surcharge de travail de la CPVP, malgré la réforme effectuée par la loi du 26 février 2003 qui est pourtant intervenue, notamment, pour alléger le travail de cette institution.

À cet égard, la CPVP a notamment souligné une caractéristique qui la distingue de la section de législation du Conseil d'État, elle aussi investie d'une large compétence d'avis. La CPVP affirme ainsi qu'elle « siège normalement toutes les trois semaines. Il ne faut toutefois pas [...] perdre de vue que les commissaires, à l'exception du président et du vice-président, remplissent cette fonction en plus de leurs missions et tâches régulières, contrairement à des organes consultatifs qui peuvent siéger de manière permanente parce que leurs membres sont à disposition de l'institution sur une base permanente, comme la section de législation du Conseil d'État »[1874].

526.- L'examen de fond des normes. Les avis de la CPVP sont principalement consacrés à l'analyse du contenu des normes qui règlementent l'administration électronique. Ils livrent l'interprétation à donner aux exigences du régime de la protection des données à caractère personnel en général et de la loi du 8 décembre 1992 en particulier et confrontent les normes en projet à chacune de celles-ci.

[1873] Entre autres exemples, le Président de la Chambre des représentants a récemment demandé à la CPVP si la publication, sur internet, des feuilletons de pétitions détenus par la Chambre porterait atteinte à la loi du 8 décembre 1992 (voy. l'avis n° 01/2012 du 18 janvier 2012 sur la publicité des feuilletons de pétitions de la Chambre des représentants).

[1874] CPVP, avis n° 31/2006 du 26 juillet 2006 relatif à la proposition de loi réglant l'installation et l'utilisation de caméras de surveillance, p. 9, note 15.

Ainsi, comme l'ont montré les deux premiers titres de la recherche, les avis de la CPVP sont d'une grande utilité pour interpréter les exigences cardinales du régime de protection des données à caractère personnel. On pense principalement à l'exigence de finalité, de proportionnalité et de légitimité, que doit respecter le législateur lorsqu'il met en place un nouveau traitement de données, ou une administration lorsqu'elle collecte ou communique des données. On pense également aux réflexions menées au sujet de l'identification du responsable de traitement et aux obligations qui s'imposent à lui pour assurer la transparence des traitements effectués.

Les avis de la CPVP viennent utilement se greffer sur les enseignements de la section de législation du Conseil d'État. Ils corroborent ainsi le constat selon lequel les exigences de la protection de la vie privée renforcent les principes de droit administratif applicables à la matière.

> Par exemple, lorsque le législateur souhaite mettre en place une nouvelle base de données, la section de législation du Conseil d'État le rend attentif au fait que l'objectif pour lequel la base de données est créée, c'est-à-dire, sa finalité, doit figurer dans la loi. Il s'agit, en effet, d'un élément essentiel du traitement de données, qui doit être prévu par le législateur en vertu de l'article 22 de la Constitution[1875].
>
> La jurisprudence de la CPVP complète judicieusement cette affirmation en offrant au législateur des indications sur la manière de définir une finalité respectueuse des exigences de protection des données. Ainsi soutient-elle notamment que la finalité doit entrer dans les missions de l'administration responsable de la base de données créées, constituer une fin en soi et être décrite à l'aide d'un critère fonctionnel[1876].

§2. La portée de l'avis

527.- Saisine et effet. La saisine de la CPVP est tantôt obligatoire, tantôt facultative. Les avis qui s'en suivent ne sont pas contraignants.

1. La saisine facultative ou obligatoire de la CPVP

528.- Saisine facultative. En général, l'avis de la CPVP est facultatif, en ce sens qu'il est émis à l'initiative de la CPVP elle-même, ou « sur demande du Gouvernement, des Chambres législatives, des Gouvernements de communauté ou de région, des Parlements de communauté ou de région, du Collège réuni ou de l'Assemblée réunie visés à l'article 60 de

[1875] Voy. *supra,* n° 103.-
[1876] Voy. *supra,* n° 120.-

la loi spéciale du 12 janvier 1989 relative aux institutions bruxelloise ou d'un comité de surveillance », comme le prévoit l'article 29, §1, de la loi du 8 décembre 1992.

Par exemple, l'obtention de l'avis de la CPVP n'est pas obligatoire lors de l'élaboration d'une norme de valeur législative, contrairement à l'avis de la section de législation du Conseil d'État qui est requis, rappelons-le, pour les avant-projets de loi, de décret et d'ordonnance, ainsi que les projets de normes de valeur réglementaire.

529.- Saisine obligatoire. La consultation de la CPVP peut être requise par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

Diverses normes prévoient aujourd'hui une telle obligation. Il s'agit, le plus souvent, d'imposer au Roi la consultation de la CPVP à l'occasion de l'adoption d'arrêtés royaux pris en exécution d'une loi organisant un traitement de données à caractère personnel.

Par exemple, la loi du 8 décembre 1992 prévoit, en son article 13, que le Roi peut déterminer les modalités d'exercice du droit d'accès indirect des citoyens à leurs données à caractère personnel, après avoir obtenu l'avis de la CPVP.

L'avis de la CPVP est également requis en vertu de l'article 17, §8, de cette même loi, qui habilite le Roi à exempter certaines catégories de responsables de traitement, de l'obligation de déclarer les traitements de données effectués.

Des lois sectorielles prévoient également une saisine obligatoire de la CPVP. Ainsi en est-il par exemple de la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale, qui prévoit, en son article 18, que le Roi peut étendre le réseau de la sécurité sociale à d'autres institutions, à la condition d'obtenir l'avis de la CPVP.

Par souci de précision, signalons que, jusqu'à la création du Comité sectoriel du Registre national en 2003[1877], la CPVP a également exercé une compétence d'avis spécifique, organisée par la loi du 8 août 1983 sur le Registre national[1878], qui explique l'abondance des avis relatifs à cette source authentique.

[1877] Loi du 25 mars 2003 modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.,* 28 mars 2003.

[1878] Pour de plus amples détails à ce sujet, voy. P. DEJAEGERE, « De raadgevende commissie voor de bescherming van de persoonlijke levenssfeer : vijf jaar werking en 'rechtspraak' », *T.B.P.,* 1990, pp. 242-251.

> Ainsi, le Roi devait obligatoirement demander l'avis de la CPVP pour étendre l'accès au Registre national à des organismes remplissant des missions d'intérêt général et pour autoriser l'utilisation du numéro d'identification au Registre national. L'avis de la CPVP était également requis pour obliger les communes à transmettre certaines informations qui ne se trouvaient pas au Registre national[1879]. Ces tâches sont aujourd'hui exercées par le comité sectoriel du Registre national, au travers des autorisations et des avis émis par celui-ci[1880].

530.- Pour une extension de la saisine obligatoire. La saisine facultative de la CPVP semble contraire à la directive 95/46. En effet, cette dernière affirme en son article 28, §2, que « chaque État membre prévoit que les autorités de contrôles sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard des traitements de données à caractère personnel ». Cette formulation érige donc la consultation de l'autorité de protection des données en une obligation et non une simple possibilité. Cette consultation devrait valoir tant pour les normes législatives que les normes de valeur réglementaire.

Par ailleurs, l'obligation de consulter la CPVP se justifie également par rapport à la raison d'être de cette institution. Créée pour veiller au respect de la protection de la vie privée et des données à caractère personnel, la CPVP doit pouvoir exercer sa compétence d'avis de manière assez effective. Dès lors, si son intervention n'est pas suffisamment sollicitée, le contrôle en vue duquel elle a été instituée n'est pas exercé. C'est d'ailleurs en ce sens que se sont déjà prononcés la section de législation du Conseil d'État, suivie de la CPVP. Selon ces autorités, la CPVP doit pouvoir exercer effectivement sa compétence d'avis par rapport à toute question relative à la protection de la vie privée.

> La section de législation du Conseil d'État et la CPVP soutiennent ainsi, à propos d'une loi relative à la protection de la vie privée contre les écoutes téléphoniques notamment, qu'il « semble requis que la Commission puisse accomplir ses missions d'avis sur toute question relative à l'application du projet de loi lorsqu'il aura été adopté, et, notamment, que le Ministre soit tenu de demander à la Commission un avis sur les projets d'arrêtés d'exécution de la loi en projet. Ce serait sinon faire échapper une partie importante de la vie privée du champ de compétences de la Commission dont le

[1879] Art. 5, 6 et 8 de la loi du 8 août 1983 organisant un registre national des personnes physiques, avant sa modification par la loi du 25 mars 2003 précitée.

[1880] Voy. les art. 5, 8, 10, 15 et 16 de la loi du 8 août 1983, depuis sa modification par la loi du 25 mars 2003 précitée.

> législateur a pourtant entendu faire une pièce majeure du système de protection de la vie privée en Belgique »[1881].

2. Le caractère non contraignant de l'avis

531.- Des avis non contraignants. Que l'avis de la CPVP soit requis, ou non, les remarques formulées par cette autorité consultative ne doivent pas nécessairement être suivies.

Pour l'heure, la CPVP semble assez satisfaite du suivi réservé à ses avis.

> Ainsi, dans son rapport d'activité de l'année 2010, la CPVP explique que, parmi les initiatives réglementaires ayant été soumises à l'avis de la CPVP, six d'entre elles ont ensuite été soumise à une évaluation. « Il est ressorti de l'analyse que le législateur a largement tenu compte des remarques/suggestions de la Commission. Les modifications apportées ont toutes eu un effet neutre ou positif en termes d'impact sur la vie privée »[1882].

Néanmoins, il ne s'agit là que d'une pratique qui ne perdurera pas nécessairement. Or, comme dit précédemment, le non respect des exigences de protection de la vie privée que dénonce bien souvent la CPVP peut porter atteinte à la constitutionnalité des normes de valeur législative et à la légalité et la constitutionnalité des normes de valeur réglementaire. Ces règles risquent alors subir la sanction de l'annulation par la Cour constitutionnelle ou le Conseil d'État. Un juge judiciaire peut également être amené à ne pas les appliquer, en vertu du mécanisme de la question préjudicielle ou de l'exception d'illégalité organisée par l'article 159 de la Constitution.

Dès lors, pour éviter la perte de temps et d'énergie que constitue l'élaboration d'une norme inconstitutionnelle vouée à disparaître de l'ordonnancement juridique, il serait judicieux de prévoir l'obligation, pour le législateur et pour le Roi, d'énoncer, dans l'exposé des motifs, les raisons qui justifient que l'avis de la CPVP ne soit pas suivi.

[1881] SLCE, avis du 15 juin 1992 sur un projet de loi relative à la protection de la vie privée conter les écoutes, enregistrements et interceptions de propos et de communications privées, *Doc. Parl.,* Sénat, sess. 1992-1993, n° 843/1, pp. 46 et 47, repris par la CPVP dans son avis n° 23/93 du 14 décembre 1993 concernant un projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, p. 5.

[1882] CPVP, rapport d'activité 2010, *op. cit.,* p. 18.

B. Le contrôle des traitements de données en cours : les recommandations et les autorisations

532.- Les traitements de données en cours. Dans les lignes qui suivent, on qualifie de traitements de données en cours, les traitements qui sont déjà encadrés par des normes législatives et réglementaires et qui sont effectués concrètement ou le seront très prochainement[1883]. Les recommandations et les autorisations encadrent le déploiement effectif de ces traitements de données.

§1. Les recommandations

533.- Articles 30 et 31 de la loi du 8 décembre 1992. En vertu de l'article 30 de la loi du 8 décembre 1992, la CPVP est compétente pour rendre des recommandations dans les mêmes hypothèses que celles qui encadrent sa compétence d'avis[1884].

> Ainsi, l'article 30, §1, de la loi du 8 décembre 1992 affirme que « la Commission peut émettre, soit d'initiative, soit sur demande du Gouvernement, des Chambres législatives, des Gouvernements de communauté ou de région, des Parlements de communauté ou de région, du Collège réuni ou de l'Assemblée réunie visés à l'article 60 de la loi spéciale du 12 janvier 1989 relative aux institutions bruxelloises ou d'un comité de surveillance, des recommandations sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel ».

Rappelons[1885] également que l'article 31 de la loi du 8 décembre 1992 prévoit que, saisie d'une plainte, la CPVP doit tenter de concilier les parties concernées. En cas d'échec de la conciliation, elle rend un avis qui

[1883] Cette hypothèse vise les autorisations des comités sectoriels : le traitement de données est organisé par une norme de valeur législative, mais une autorisation est nécessaire pour effectuer concrètement l'émission des données depuis la source authentique qui les détient.

[1884] Nombre de recommandations concernent les traitements ultérieurs de données non codées à des fins historiques, statistiques ou scientifiques. Ces recommandations sont obligatoires (art. 21 de l'arrêt royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel). Néanmoins, nous n'analysons pas cette problématique dans le cadre de la présente recherche.

[1885] Voy. *supra,* n° 478.-

peut être assorti de recommandations à l'intention du responsable de traitement.

Dans ses recommandations, la CPVP n'analyse pas un projet de norme. Elle se prononce sur la légalité d'une pratique de traitements de données au regard des normes y applicables et suggère des solutions qui, souvent, orientent utilement les responsables de traitement face au flou législatif en matière d'e-gouvernement[1886].

Les recommandations peuvent s'adresser à un responsable de traitement en particulier, pour l'aider à respecter les exigences du régime de la protection des données à caractère personnel. Dans ce cas, la loi prévoit que la Commission doit donner à ce dernier « l'occasion de faire connaître son point de vue »[1887].

> Par exemple, récemment, la CPVP a émis une recommandation relative aux « principes de base à respecter lors de traitements et d'échanges de données impliquant le SPF Finances », partant du constat que « la pratique a démontré que les compétences actuelles du comité [sectoriel pour l'Autorité fédérale] ne sont pas suffisantes pour permettre de dégager des solutions pour des questions concernant les échanges de données auxquels le SPF Finances est confronté dans son fonctionnement au quotidien » et, plus précisément, les échanges de données entre les services internes du SPF Finances[1888]. Cette recommandation se fonde sur une note transmise par ce SPF.

Les recommandations peuvent également avoir un champ d'étude plus large et viser une catégorie de traitements qui nécessitent un éclairage particulier. En général, ces recommandations font le point sur des outils importants de l'e-gouvernement qui posent des difficultés récurrentes. La CPVP estime nécessaire de se prononcer à leur sujet, soit qu'elle ait reçu de nombreuses questions à leur égard, soit qu'elle ait constaté, dans l'exercice de sa compétence d'avis, l'importance d'apporter certains éclaircissements.

> À cet égard, on a déjà souligné l'importance de la recommandation relative aux intégrateurs dans le service public[1889] et celle concernant les sources

[1886] Dans la mesure où, le plus souvent, les recommandations visent des traitements de données déjà en cours, nous avons choisi de traiter de cette question dans ce chapitre, sans exclure toutefois le constat selon lequel ces recommandations ont vocation à améliorer la légalité de traitements en projet.

[1887] Art. 30, §2, de la loi du 8 décembre 1992.

[1888] Recommandation n° 02/2012 du 8 février 2012 relative aux principes de base à respecter lors de traitements et d'échanges de données impliquant le SPF Finances, n° 3.

[1889] Recommandation d'initiative n° 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public.

authentiques de données[1890], qui sont deux outils fondamentaux dans l'e-gouvernement dont la réglementation subit, pour l'heure, d'importantes lacunes législatives. Par ces recommandations, la CPVP apporte des définitions claires et analyse les conditions de leur légalité.

§2. Les autorisations

534.- Les comités sectoriels. Les autorisations de la CPVP sont rendues par des comités sectoriels institués en son sein[1891].

L'article 31*bis* de la loi du 8 décembre 1992 définit les comités sectoriels comme les autorités compétentes « pour instruire et statuer sur des demandes relatives au traitement ou à la communication de données faisant l'objet de législations particulières, dans les limites déterminées par celles-ci ». En somme, par ces autorisations, le comité sectoriel compétent décide si des données détenues par une administration peuvent être communiquées à celui qui les demande. Le comité sectoriel intervient lorsque la demande porte sur l'accès à des données à caractère personnel, comme c'est le cas par exemple lorsque le SPF Finances demande au Registre national la mise à jour de l'adresse d'un contribuable. Par contre, s'il s'agit d'accéder à un document qui contient des données à caractère personnel, mais non aux données elles-mêmes, on appliquera la loi du 7 mars 2007 sur la réutilisation des informations du secteur public qui prévoit que lorsque le document réutilisé contient des données à caractère personnel, il doit être anonymisé[1892].

[1890] Recommandation d'initiative n° 09/2012 du 23 mai 2012 relative aux sources authentique de données dans le secteur public.

[1891] La présente partie de la recherche se concentre sur les comités sectoriels institués au niveau fédéral. Progressivement, les communautés et les régions se dotent d'un pareil outil de contrôle. Ainsi, le décret flamand du 18 juillet 2008 sur l'échange électronique de données administratives institue une « commission de contrôle » flamande, calquée sur le modèle des comités sectoriels. Un projet de décret wallon prévoit une autorité semblable également. À ce sujet, voy. Y. Poullet et E. Degrave, « La création d'une institution en charge de la protection des données au sein de la Communauté française et/ou de la Région wallonne », *R.D.T.I.,* 2008, pp. 427-429.

[1892] Loi du 7 mars 2007 transposant la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *M.B.,* 19 avril 2007. Nous n'étudions pas cette loi dans le cadre de la présente recherche étant donné que nous nous concentrons sur la manière d'assurer la circulation des données à caractère personnel non anymisées au sein de l'administration. Au sujet des interactions entre la loi du 8 décembre 1992 et ladite loi du 7 mars 2007, voy. C. de Terwangne et J.-P. Moiny, « À la croisée de la publicité de l'administration, de la réutilisation des informations du secteur public et de la protection des données : l'exemple de la directive INSPIRE », *C.D.P.K.,* 2010, pp. 121 à 141.

La création des comités sectoriels répond au souci de la directive 95/46 de garantir, dans chaque État-membre, l'existence d'une ou de plusieurs autorité(s) de contrôle disposant notamment de « pouvoirs effectifs d'intervention », tels que celui « d'interdire temporairement ou définitivement un traitement »[1893]. Cette exigence est également consacrée par Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) concernant les autorités de contrôle et les flux transfrontières de données, du 8 novembre 2001.

> Ce protocole additionnel affirme, en son article premier, que les autorités de contrôle nationales doivent disposer d'un pouvoir effectif. Le rapport explicatif de ce protocole indique que « la liste des pouvoirs attribués à l'autorité de contrôle par l'article 1, paragraphe 2, [du Protocole additionnel], n'est pas exhaustive » que « les Parties possèdent des possibilités supplémentaires pour donner effet à la mission de l'autorité de contrôle ». Par exemple, « l'autorité de contrôle pourrait être habilitée à procéder à des contrôles préalables sur la légitimité d'opérations de traitements »[1894].

Compte tenu du fait que, depuis la réforme législative de 2003, les comités sectoriels sont institués au sein de la CPVP, cette dernière est désormais dotée d'un pouvoir de décision, tout en étant également soumise à une exigence d'indépendance. Les développements consacrés au statut de la CPVP ont souligné les difficultés que l'attribution d'un tel pouvoir de décision génère, tant au regard de la Constitution belge, que du droit européen.

Dans la lignée de ces réflexions, la présente partie de la recherche est consacrée à la raison d'être et à l'historique des comités sectoriels, ainsi qu'à leur fonctionnement. Elle aboutit à la question de savoir si le maintien de ces organes est nécessaire.

1. La raison d'être et l'historique des comités sectoriels

535.- Considérations générales. Le premier comité sectoriel a été institué pour vérifier la légalité des transferts de données au sein du réseau de la sécurité sociale. Ce modèle s'est ensuite étendu à d'autres secteurs, et les compétences des comités sectoriels se sont déployées.

[1893] Art. 28, §2, de la Directive 95/46. Voy. égal. le considérant 62 de ladite Directive.

[1894] Rapport explicatif du Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données STE n° 181, point 16, disponible sur le site http://conventions.coe.int/Treaty/FR/reports/Html/181.htm.

a) La raison d'être des comités sectoriels

536.- Les contrôleurs de la légalité des transferts de données. La création des comités sectoriels poursuit *a priori* un objectif légitime, celui du contrôle de la légalité des transferts de données, au cas par cas et par des spécialistes du secteur dans lequel les échanges de données ont lieu. C'est l'idée que des personnes du terrain peuvent ainsi veiller à ce que les traitements de données accomplis dans l'administration respectent tant la loi que les préoccupations concrètes de l'administration.

> Comme l'a affirmé la CPVP pour souligner l'intérêt des comités sectoriels, « ces organes de contrôle spécifiques [...] dans lesquels siégeraient, entre autres, des représentants du secteur concerné, devraient s'attacher à rechercher des solutions concrètes à des problèmes concrets » et « exercer un contrôle 'de première ligne' dans le domaine de la protection des données à caractère personnel »[1895]. Et d'ajouter que « l'existence de ces organes au sein du secteur concerné entraîne une sensibilité accrue aux risques pour la vie privée issus du traitement de données à caractère personnel »[1896].

Ce n'est d'ailleurs pas un hasard que le premier comité du genre ait vu le jour en 1990, au moment de la création de la Banque-Carrefour de la sécurité sociale[1897]. Comme cela a été dit à plusieurs occasions, la loi du 15 janvier 1990[1898] crée la Banque-Carrefour de la sécurité sociale pour faciliter, et donc encourager, les transferts de données entre les institutions de sécurité sociale. Plus encore, elle impose de tels transferts, au travers de l'obligation de collecte unique des données. Il est alors apparu essentiel d'instituer, au sein de la Banque-Carrefour de la sécurité sociale, un organe de contrôle des transferts de données.

> Ainsi, la loi du 15 janvier 1990 dans sa version initiale institue, auprès de la Banque-Carrefour de la sécurité sociale, le Comité de surveillance de la Banque-Carrefour de la sécurité sociale[1899]. Dans les discussions préparatoires à l'adoption de la loi, il est affirmé qu' « il s'agit de considérer l'installation du Comité de surveillance comme le préalable indispensable à la mise en fonctionnement de la Banque-Carrefour »[1900]. Ce comité, chargé d'autoriser « toute communication dans le réseau de données sociales à

[1895] CPVP, avis n° 30/96, *op. cit.*, n° 60.
[1896] *Ibid.*, n° 62.
[1897] Voy. *supra*, n° 492.-
[1898] Loi du 15 janvier 1990, relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *Pasin.*, 1990, I, pp. 58 et s.
[1899] Art. 37 de la loi du 15 janvier 1990.
[1900] Rapport fait au nom de la Commission des affaires sociales par Mme Nelis-Van Liedekerke, *Doc. Parl.*, Ch. Repr., session 1988-1989, n° 899/4, repris dans *Pasin.*, 1990, I, p. 130.

caractère personnel, par la Banque-Carrefour ou les institutions de sécurité sociale »[1901], « examinera à cette occasion si les conditions définies par la loi [...] quant à la légalité de ce transfert de données, sont remplies »[1902].

Néanmoins, comme on l'a dit à plusieurs occasions, les normes qui organisent la protection des données sont bien souvent floues et lacunaires. Leur application à des transferts concrets de données suppose quasi nécessairement que les comités sectoriels contribuent à définir plus précisément la norme applicable. Les décisions des comités sectoriels font alors partie des règles applicables aux traitements de données dans l'administration, ce que la CPVP semble admettre en reconnaissant aux décisions des comités sectoriels la valeur de « dispositions réglementaires »[1903]. Une telle compétence confiée aux comités sectoriels pose question, notamment parce que le pouvoir de décision des ces autorités n'est encadré d'aucun critère légal, comme l'a dénoncé la section de législation du Conseil d'État[1904].

b) L'historique des comités sectoriels

537.- La multiplication des comités sectoriels. Le Comité de surveillance de la Banque-Carrefour de la sécurité sociale séduit car il semble constituer un mode de contrôle rapide et précis de la protection de la vie privée menacée par le développement de l'e-gouvernement[1905]. C'est pourquoi, progressivement, le législateur crée d'autres comités appelés « comités sectoriels »[1906] depuis la loi du 26 février 2003 précitée.

[1901] Art. 15 de la loi du 15 janvier 1990 précitée.

[1902] Projet de loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, Commentaire des articles, *Doc. Parl.,* Ch. Repr., session 1988-1989, n° 899/1, repris dans *Pasin.,* 1990, I, p. 84.

[1903] Voy. *infra,* n° 543.-

[1904] *Idem.*

[1905] CPVP, avis n° 43/2006 du 8 novembre 2006 concernant une demande d'avis du Ministre de l'Emploi et de l'Informatisation relatif à un projet de loi portant dispositions diverses – création d'un comité sectoriel de la sécurité sociale et de la santé, n° 5.

[1906] Signalons que, ici aussi, le législateur a manqué d'uniformiser les concepts. Ainsi, certains comités sont dénommés « comité sectoriel » tandis que d'autres sont qualifiés de « comité de surveillance ». Nous utilisons néanmoins les termes « comités sectoriels » comme concept générique pour qualifier ces organes de la CPVP.

Il existe ainsi le Comité sectoriel de la Banque-Carrefour des Entreprises[1907], le Comité sectoriel du Registre national[1908], le Comité sectoriel pour l'Autorité Fédérale ainsi que le Comité de surveillance sectoriel « Phenix » dans le secteur judiciaire[1909], et le Comité de surveillance Statistique[1910]. Par ailleurs, le Comité de surveillance de la Banque-Carrefour de la sécurité sociale s'est mué en Comité sectoriel de la sécurité sociale et de la santé[1911].

L'idée est alors d'instituer des contrôleurs pour chaque secteur de l'administration organisé par une loi particulière. Un comité doté d'une compétence résiduaire est également créé, le comité sectoriel pour l'Autorité fédérale. Il est chargé de contrôler les transferts de données qui ne relèvent d'aucune loi particulière.

Néanmoins, cette multiplication d'autorités de contrôle fait progressivement apparaître des difficultés. D'une part, aucune ligne directrice ne semble établie, qui guiderait la mise en place uniforme des comités sectoriels, ce qui pose problème pour définir le comité sectoriel compétent à l'égard de certains transferts de données[1912]. On constate ainsi que certains comités sectoriels sont créés pour contrôler les administrations qui appartiennent à un réseau sectoriel défini. Il s'agit du Comité sectoriel de la sécurité sociale et de la santé, section sécurité sociale, qui est compétent pour contrôler les institutions de sécurité sociale faisant partie du réseau de la sécurité sociale. Récemment, une tentative a été faite de créer un Comité sectoriel « Mobilité et Transports », pour contrôler les institutions liées à la Banque-Carrefour des véhicules[1913]. Par contre, d'autres comités sectoriels sont créés pour être les « chiens de garde » d'une source authentique de données, comme le Comité sectoriel Phénix, le Comité sectoriel du Registre national et le Comité sectoriel de la Banque-Carrefour des

[1907] Art. 27 à 32 de la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises [...] ; Arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP.

[1908] Art. 5 de la loi du 8 août 1983 organisant un registre national des personnes physiques ; Arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la CPVP.

[1909] Art. 22 à 26 et 28 de la loi du 10 août 2005 instituant le système d'information Phenix.

[1910] Art. 24*sexies* à 24*octies* de la loi du 4 juillet 1962 relative à la statistique publique, *M.B.,* 20 juillet 1962.

[1911] Art. 37 à 52 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale. Voy. D. De Bot, *op. cit.,* p. 399.

[1912] Voy. *infra,* n° 547.-

[1913] À ce sujet voy. CPVP, avis n° 23/2008 avant-projet de loi portant création de la source authentique des données relatives aux véhicules, n° 73 et s.

entreprises[1914]. C'est également le cas du Comité sectoriel de la sécurité sociale et de la santé, section santé.

D'autre part, la multiplication de comités sectoriels nuit à « la transparence, la sécurité juridique et l'unité de jurisprudence »[1915]. Il est de plus en plus difficile de savoir à qui s'adresser et d'accéder aux autorisations rendues afin de comprendre quels échanges de données sont autorisés. C'est pourquoi, depuis quelques années, la CPVP décourage la création de nouveaux comités sectoriels lorsque leur nécessité n'est pas démontrée.

> Elle l'a fait encore récemment à propos d'un projet de Comité sectoriel « Mobilité et transports » affirmant qu' « un comité sectoriel distinct peut être justifié si un secteur déterminé connaît des besoins spécifiques au point de nécessité la création d'un comité supplémentaire »[1916].

538.- L'intégration des comités sectoriels au sein de la CPVP. Comme cela a été dit précédemment, les comités sectoriels sont intégrés au sein de la CPVP par la loi du 26 février 2003 qui opère une réforme importante de cette institution. Ce faisant, on souhaitait améliorer la cohérence des décisions des comités sectoriels et effectuer des économies d'argent public[1917]. A-t-on pourtant suffisamment perçu, à l'époque, qu'il ne s'agissait pas là d'une modification purement formelle ? On en doute.

D'une part, l'intégration des comités sectoriels à la CPVP nuit à l'indépendance de cette dernière. En effet, les comités sectoriels doivent être composés de personnes issues du secteur contrôlé, sans qui le contrôle effectué ne serait pas assez adapté aux préoccupations des administrations concernées. Comment prétendre à l'indépendance quand le contrôleur est lui-même le contrôlé ? Une critique semblable a été formulée par la section de législation du Conseil qui craint une confusion entre le rôle des comités sectoriels et celui de la CPVP.

> La section de législation du Conseil d'État affirme que, bien que l'intégration des comités sectoriels au sein de la CPVP favorise la cohérence dans l'action des ces autorités, il faut toutefois observer que « les diverses missions attribuées au Comité, d'une part, et à la Commission, d'autre part, ne permettent pas d'exclure *a priori* une certaine confusion entre les rôles respectifs de ces deux organismes, spécialement lorsque la Commission serait amenée, en sa qualité d'organe de contrôle général, à devoir se prononcer au

[1914] Rappelons que, contrairement à ce que son nom peut laisser croire, la Banque-Carrefour des entreprises est une source authentique de données.

[1915] CPVP, avis n° 23/2008 précité, n° 75. Dans le même sens, voy. CPVP, avis n° 07/2002 du 11 février 2002 relatif à un projet de loi créant une Banque-Carrefour des Entreprises.

[1916] À ce sujet voy. CPVP, avis n° 23/2008, *op. cit.*, n° 73 et s.

[1917] Voy. *supra,* n° 487.-

> sujet de décisions, d'avis ou de recommandations précédemment formulés par le Comité [...], en sa qualité d'organe de contrôle sectoriel. Il convient donc que le législateur prenne également des dispositions afin d'éviter toute discordance en la matière, de même qu'une éventuelle confusion des rôles 'contrôleur/contrôlé' »[1918].

D'autre part, l'indépendance de la CPVP nuit à la légitimité des décisions des comités sectoriels car aucun ministre n'en assume la responsabilité et qu'elles ne sont peut-être pas attaquables devant le Conseil d'État.

Rappelons[1919] que le premier comité sectoriel créé – appelé à l'époque le comité de surveillance de la Banque-Carrefour de la sécurité sociale – était un organe de l'institution publique qu'est la Banque-Carrefour de la sécurité sociale. Cet organe contrôlait les échanges de données effectués au sein du réseau de la sécurité sociale en appliquant une loi sectorielle.

À l'époque déjà, ce comité disposait du pouvoir d'exécution de la loi du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale, qui consistait à vérifier que les conditions fixées par cette loi sont concrètement respectées lors des échanges de données au sein du réseau. Néanmoins, ce pouvoir d'exécution de la loi était encadré puisqu'il était soumis au contrôle de tutelle que le Ministre des Affaires sociales exerce sur la Banque-Carrefour de la sécurité sociale[1920]. Par ailleurs, la Banque-Carrefour étant une autorité administrative, ces autorisations étaient attaquables au Conseil d'État[1921].

Aujourd'hui, le fait d'instituer les comités sectoriels au sein d'une autorité qui dont la qualité d'autorité administrative n'est pas certaine rend ses décisions difficilement contrôlables.

2. Le travail des comités sectoriels

539.- Pourquoi ? Qui ? À qui ? L'étude du travail accompli par les comités sectoriels[1922] suppose l'étude de l'objet des autorisations, l'identi-

---

[1918] SLCE, avis n° 33.962/2 précité, n° 50-2226/003, p. 10.

[1919] Voy. *supra,* n° 492.- et n° 536.-

[1920] Cela a été affirmé lors des travaux préparatoires de la loi du 15 janvier 1990 (Rapport fait au nom de la Commission des affaires sociales par Mme Nelis-Van Liedekerke précité, p.113) et confirmé par un juriste de la Banque-Carrefour de la sécurité sociale en mai 2012.

[1921] Néanmoins, nous n'avons pas connaissance de recours intentés jadis à l'encontre d'une décision du Comité de surveillance de la Banque-Carrefour de la sécurité sociale.

[1922] Les comités sectoriels sont compétents pour adopter des autorisations mais également rendre des avis et des recommandations. Néanmoins, leur fonction principale est consacrée à rendre des autorisations, compétence par ailleurs problématique. Ces deux raisons expliquent que les lignes qui suivent soient consacrées à cette compétence.

fication du comité sectoriel compétent pour octroyer chaque autorisation ainsi que les institutions soumises à l'obligation de demander un tel laissez-passer.

a) L'objet de l'autorisation

540.- Des données détenues par une administration fédérale. En principe, il y a lieu d'obtenir l'autorisation d'un comité sectoriel pour accéder à des données détenues au sein d'une administration fédérale[1923]. Il s'agit bien sûr des données enregistrées dans des bases de données ayant la qualité de source authentique. Mais il s'agit également des données qui, sans être enregistrées dans une source authentique, sont néanmoins détenues par une administration fédérale. En effet, le Comité sectoriel pour l'Autorité fédérale est compétent pour autoriser les communications électroniques des données provenant d'un service public fédéral ou d'un organisme public doté de la personnalité juridique qui relève de l'autorité fédérale[1924].

541.- Communication électroniques – communication sur papier. Les communications de données sur papier sont-elles également soumises à l'autorisation d'un comité sectoriel ? Cette question ne se pose que pour les données qui relèvent de la compétence du Comité sectoriel pour l'Autorité fédérale. Pour les autres comités sectoriels, c'est le fait que la donnée soit issue d'une source authentique ou soit transférée par l'intermédiaire d'une Banque-Carrefour qui impose l'autorisation d'un comité sectoriel, peu importe que la transmission se fasse par voie électronique ou papier[1925].

La loi précise que le Comité sectoriel pour l'Autorité fédérale est compétent pour autoriser les « communications électroniques » de données[1926]. À plusieurs reprises, ce comité sectoriel a interprété ces termes de manière

[1923] Progressivement, des autorités semblables aux comités sectoriels fédéraux sont constituées au niveau des communautés et régions pour accomplir les mêmes tâches. Voy., par exemple, l'article 11, §1, du décret flamand du 18 juillet 2008 sur l'échange électronique de données administratives et l'article 22, §1, du décret du 4 juillet 2013 portant assentement à l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française sur le développement d'une initiative commune en matière de partage des données et sur la gestion conjointe de cette initiative.

[1924] Art. 36*bis,* de la loi du 8 décembre 1992.

[1925] Voy. *infra,* n° 546.-

[1926] Art. 36*bis,* de la loi du 8 décembre 1992.

assez large, en y incluant les transferts de données effectués sur un cd-rom[1927].

Toutefois, les transferts de données par la voie du papier n'entrent pas dans ce concept. On s'en étonne, compte tenu qu'une discrimination est ainsi créée entre, d'une part, les citoyens dont les données sont transmises par voie électronique et qui bénéficient du contrôle exercé par un comité sectoriel, et, d'autre part, les individus dont le dossier circule par la voie du papier et sont dès lors privés d'un tel contrôle. En outre, la procédure d'autorisation est lourde pour les demandeurs de données. Le fait de pouvoir y échapper en ne recourant pas à l'électronique pourrait encourager les administrations à imprimer les données demandées et à les envoyer par la voie postale, ce qui ne contribuerait pas au développement de l'e-gouvernement.

542.- Le contrôle de la légalité des transferts de données. Chaque comité sectoriel est chargé de se prononcer sur la conformité, par rapport aux exigences du régime juridique de la protection des données, du transfert des données demandées. Les normes par rapport auxquelles chaque comité sectoriel doit confronter les demandes de transfert de données varient d'un comité sectoriel à l'autre, accentuant davantage encore le manque d'uniformité qui affecte les comités sectoriels.

> À titre d'exemple, le Comité sectoriel du Registre national doit confronter la demande à la loi sectorielle concernée (il s'agit de la loi du 8 août 1983 précitée) ainsi qu'à la loi du 8 décembre 1992 et ses dispositions d'exécution, et les « autres normes pertinentes en matière de protection de la vie privée ou des données à caractère personnel »[1928]. Le Comité sectoriel de la sécurité sociale et de la santé confronte seulement les demandes à la loi sectorielle concernée (il s'agit de la loi du 15 janvier 1990) ainsi qu'aux mesures d'exécution de cette dernière « en ce compris les instructions données par le comité de gestion de la Banque-Carrefour pour son application »[1929]. Le Comité sectoriel pour l'Autorité fédérale étudie la demande au regard « des dispositions légales et réglementaires »[1930], tandis que le Comité sectoriel

[1927] Voy. not. C.S.A.F., délibération n° 02/2012 relative à une demande du SPF Intérieur, Direction générale Sécurité civile, d'accéder à certaines données cadastrales (Documentation patrimoniale – SPF Finances) dans le cadre de la réforme des services de secours ; C.S.A.F., délibération 07/2007 du 2 mai 2007, relative à une demande formulée par le SPF Intérieur, Direction générale Institutions et Population, afin d'obtenir la communication de données à caractère personnel de la part du SPF P&O.

[1928] Art. 5 de la loi du 8 août 1983.

[1929] Art. 15, §1, de la loi du 15 janvier 1990.

[1930] Art. 36*bis*, de la loi du 8 décembre 1992.

pour la Banque-Carrefour des entreprises le fait par rapport à la loi sectorielle sur la Banque-Carrefour des Entreprises et ses arrêtés d'exécution[1931].

Un comité sectoriel doit donc, en principe, vérifier l'existence d'une base légale dans le chef de l'administration émettrice des données et de celle destinatrice de celle-ci, apprécier le respect d'une finalité déterminée, explicite et légitime, s'assurer de la proportionnalité du traitement et des données ainsi que la mise en œuvre des exigences de transparence et de sécurité des données[1932].

a) Une compétence problématique. Les concepts utilisés par la loi du 8 décembre 1992 sont si larges que leur application à des cas particuliers suppose quasi nécessairement que le comité sectoriel intervienne lui-même dans la définition des normes du régime de protection des données à caractère personnel. Pourtant, comme l'a rappelé à maintes reprises le titre premier de la présente recherche, la définition des éléments essentiels des traitements de données est réservée au législateur. Une partie de ce travail peut, certes, être déléguée au Roi, mais c'est à la condition que le législateur définisse lui-même les critères qui encadrent l'exercice du pouvoir exécutif.

Or, on l'a dit, le législateur n'a pas défini les critères qui encadrent le pouvoir d'appréciation des comités sectoriels, ce qui a été critiqué par la section de législation du Conseil d'État[1933]. Par ailleurs, rappelons que les comités sectoriels sont des organes de la CPVP. Ils ne font pas partie du pouvoir exécutif. Ainsi qu'on l'a déjà dit[1934], prétendre que ces autorités peuvent mettre en œuvre les lois est donc critiquable au regard des exigences constitutionnelles et, en particulier, du principe de la responsabilité du Ministre du fait de l'administration d'une part, et du principe de l'indisponibilité des compétences, d'autre part.

b) La position critiquable de la CPVP. Malgré ces difficultés, la CPVP confère de plus en plus d'importance à la compétence décisionnelle des comités sectoriels.

Dans une recommandation récente sur les sources authentiques, elle considère que le législateur ne doit pas énumérer de manière exhaustive l'ensemble des finalités de la source authentique dès sa création. En effet, selon la CPVP, si, ultérieurement, on souhaite utiliser les données de la source authentique pour une nouvelle finalité, les comités sectoriels « peuvent d'ailleurs – pour autant que cela n'aille pas à l'encontre

[1931] Art. 18, §2, de la loi du 16 janvier 2003.
[1932] Voy. *supra,* Titre I.
[1933] SLCE, avis n° 33.962/2 précité, n° 50-2226/003, p. 6.
[1934] Voy. *supra,* n° 508.- et s.

de dispositions réglementaires existantes – déclarer aussi eux-mêmes un traitement ultérieur comme étant compatible. Une autorisation constitue en effet une décision normative qui est rendue publique de sorte que de telles décisions peuvent être considérées comme une 'disposition réglementaire' au sens de l'article 4, § 1, 2° de la LVP ». La CPVP semble donc considérer qu'une décision d'un comité sectoriel rendue publique s'apparente nécessairement à une disposition adoptée par le pouvoir exécutif dans le cadre de son pouvoir d'exécuter les lois. C'est oublier que les comités sectoriels ne font pas partie du pouvoir exécutif.

La position de la CPVP est critiquable et pourrait mener à des dérives. En effet, comme en atteste le deuxième titre de la recherche consacré à la transparence, les administrations peuvent, dans certaines hypothèses, être dispensées de l'obligation de déclarer les traitements de données qu'elles effectuent. Ces hypothèses sont définies largement par l'article 61 de l'arrêté royal du 13 février 2001[1935].

> Cette disposition affirme qu' « à l'exception des paragraphes 4 et 8, l'article 17 de la loi n'est pas applicable aux traitements de données à caractère personnel effectués par des autorités administratives si le traitement est soumis a` des réglementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées ainsi que leur utilisation et leur obtention ».

Puisque la CPVP estime que les décisions de comités sectoriels constituent des dispositions règlementaires, n'y-t-il pas un risque que, tôt ou tard, elle en vienne à soutenir que les décisions rendues par les comités sectoriels constituent une « réglementation particulière » adoptée « en vertu de la loi et réglementant l'accès aux données traitées ainsi que leur utilisation et leur obtention » ? Si tel était le cas, les administrations soumises à une décision de comité sectoriel ne seraient plus soumises à l'obligation de déclaration, ce qui reviendrait à accentuer encore davantage l'opacité des traitements de données effectués au sein de l'administration.

Ce serait d'autant plus problématique que les décisions des comités sectoriels sont elles-mêmes peu transparentes, la prise de connaissance de cette jurisprudence s'apparentant à un véritable parcours du combattant. Certes, les avis sont accessibles sur le site internet de la CPVP. Mais ils sont extrêmement nombreux et accessibles principalement à partir de leur date[1936]. En outre, la structure ainsi que le raisonnement suivis

[1935] Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à` la protection de la vie privée à l'égard des traitements de données à caractère personnel.

[1936] Le site de la CPVP prévoit une recherche par mots-clés, mais celle-ci s'avère peu efficace.

divergent d'un comité sectoriel à l'autre, voire d'une demande à l'autre. C'est d'autant plus problématique que les normes organisant la protection des données à caractère personnel sont floues à bien des égards, ce qui laisse une marge d'appréciation importante aux comités sectoriels chargés de les appliquer. Par ailleurs, ni la CPVP elle-même, ni les comités sectoriels ne publient d'analyse de cette jurisprudence. Il serait pourtant fort utile de disposer d'un document classant ces décisions par problématique, par exemple. Dès lors, il est très difficile, voire impossible, de comprendre la jurisprudence de chaque comité sectoriel, ce qui doit être particulièrement décourageant pour une administration désireuse d'accomplir ses missions à bien et souhaitant introduire une demande d'autorisation de la manière la plus efficace possible[1937].

543.- Exceptions et tempérament. Tous les transferts de données ne doivent pas être autorisés par un comité sectoriel. En effet, la loi du 8 décembre 1992 et les législations sectorielles organisent des exceptions à l'obligation d'obtenir l'autorisation d'un comité sectoriel. Par ailleurs, la possibilité de rallier une autorisation générale apporte un tempérament à cette procédure.

a) Exceptions. Le Roi peut organiser des exceptions à l'obligation de demander l'autorisation d'un comité sectoriel, comme le prévoient la loi du 8 décembre 1992 et les législations sectorielles instituant un comité sectoriel.

> Tel est le cas pour le Comité sectoriel pour l'Autorité fédérale, le Comité sectoriel du Registre national, le Comité sectoriel de la sécurité sociale et de la santé et le Comité sectoriel de la Banque-Carrefour des entreprises. Cette prérogative n'est pas déléguée au Roi s'agissant du Comité sectoriel Phénix et du Comité sectoriel Statistique.

La délégation de cette compétence au Roi est critiquable. Ainsi, à trois reprises, la section de législation du Conseil d'État a affirmé qu'une telle compétence confiée au Roi est anticonstitutionnelle, à défaut pour le législateur d'avoir fixé les critères devant guider les arrêtés royaux adoptés dans ce cadre.

[1937] Signalons toutefois l'existence de formulaires pour introduire les demandes d'autorisation qui sont disponibles sur le site de la CPVP, dans la rubrique « demander une autorisation », qui renvoie à une rubrique par comité sectoriel. Par exemple, le formulaire pour les autorisations d'accès au Registre national est disponible à l'adresse suivante http://www.privacycommission.be/sites/privacycommission/files/documents/formulaire-demande-autorisation-rn.pdf

Selon la section de législation du Conseil d'État, la disposition législative prévoyant que le Roi est compétent pour fixer, dans un arrêté délibéré en Conseil des ministres, les cas dans lesquels l'accès aux informations du Registre national n'est pas soumis à une autorisation du Comité d'habilitation pour le Registre national[1938] n'expose pas « concrètement en quoi consiste l'habilitation ainsi conférée au Roi ». « La compétence ainsi déléguée au Roi est définie en termes trop généraux et le législateur doit déterminer lui-même les éléments essentiels de cette dérogation ou, à tout le moins, préciser les critères sur la base desquels le Roi pourra exercer les compétences qui Lui sont attribuées. À défaut de telles précisions, les garanties prévues par le projet perdraient le caractère intangible que l'intervention du législateur est censée leur procurer et la délégation de pouvoir ainsi consentie ne saurait se concilier avec l'article 22 de la Constitution »[1939].

La même critique a été adressée à la loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale[1940] et à la loi portant création d'une Banque-Carrefour des Entreprises[1941].

b) Tempérament. Les autorisations générales. Une administration ne doit pas nécessairement suivre l'entièreté de la procédure d'autorisation. En effet, les comités sectoriels adoptent des autorisations qualifiées de « générales ». Ces autorisations ne sont pas adressées à un bénéficiaire en particulier. Elles fixent les conditions d'utilisations de données ayant vocation à répondre à un besoin dans plusieurs organismes publics ou privés.

Par exemple, une autorisation générale adoptée par le Comité sectoriel du Registre national porte « autorisation unique d'accès au Registre national des personnes physiques et d'utilisation du numéro du Registre national des

[1938] Appelé aujourd'hui « Comité sectoriel du Registre national ».

[1939] Avis L. 33.962/2 du 19 novembre 2002 sur un avant-projet de loi modifiant la loi du 8 août 19 83 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *op. cit.*, pp. 57-58.

[1940] Voy. l'avis du 27 avril 1989 sur un projet de loi instituant une Banque-Carrefour de la sécurité sociale, *op. cit.*, pp. 101 et 102. Signalons que cette disposition, comme d'autres critiquées pour les mêmes raisons, figure pourtant dans la loi (Voy. l'art. 15 de la loi relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.*, 22 février 1990).

[1941] Voy. l'avis L. 33.285/1 du 2 mai 2202 sur un avant-projet de loi portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce et création des guichets d'entreprises, *Doc. Parl.*, Chambre, session 2002-2003, n° 50-2058/001, p. 103. Signalons que cette disposition figure pourtant dans la loi (Voy. l'art. 18, § 2, de la loi portant création d'une Banque-Carrefour des Entreprises, modernisation du registre du commerce, création de guichets-entreprises agréés et portant diverses dispositions, *M.B.*, 5 mai 2003).

> personnes physiques par les organes de l'État, des Communautés et Régions et des organismes de droit public, tenus d'accorder eux-mêmes les allocations familiales aux membres du personnel »[1942]

Les bénéficiaires potentiels de l'autorisation générale doivent seulement établir qu'ils répondent aux conditions fixées par le comité sectoriel en remplissant un engagement de conformité mis à leur disposition sur le site internet de la CPVP.

b) Le demandeur de l'autorisation

544.- La limitation des demandeurs. En principe, toute personne ou institution qui souhaite accéder à des données détenues par l'administration est tenue de demander l'autorisation au comité sectoriel compétent. Néanmoins, certaines lois limitent d'emblée l'accès aux données à certaines institutions. En d'autres termes, si le demandeur d'une autorisation n'entre pas dans l'un des catégories prévues par la loi, sa demande sera déclarée irrecevable.

Une telle limitation est organisée pour l'accès au Registre national, à la Banque-Carrefour des entreprises, et aux données transférées par l'intermédiaire de la Banque-Carrefour des véhicules.

c) L'émetteur de l'autorisation

545.- L'objet de la compétence de chaque comité sectoriel. Chaque comité sectoriel dispose d'une compétence propre.

Le Comité sectoriel de la sécurité sociale et de la santé est divisé en deux sections : la section « sécurité sociale » et la section « santé ».

La section « sécurité sociale » est compétente, d'une part, pour « l'examen des dossiers concernant le traitement [...] de données à caractère personnel au sens de la loi du 8 décembre 1992 [...] », effectué « par les institutions de sécurité sociale[1943] et les personnes [...] [visées à] l'article 18 [de la loi sur la Banque-Carrefour de la sécurité sociale] »[1944]. D'autre part, cette section est compétente pour « l'examen de dossiers concernant le traitement de données sociales à caractère personnel[1945] par les instances

[1942] Délibération RN n° 15/2009 du 18 février 2009.

[1943] Ce terme doit être compris au sens de l'art. 2, 2°, de la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale (ci-après « loi du 15 janvier 1990 »).

[1944] Art. 43*bis*, al. 1, de la loi du 15 janvier 1990.

[1945] Cette notion doit être comprise au sens de l'art. 2, 6°, de la loi du 15 janvier 1990, qui définit les données sociales à caractère personnel comme « toutes données sociales concernant une personne (physique) identifiée ou identifiable ».

d'octroi visées à l'article 11*bis*, [de la loi sur la Banque-Carrefour de la sécurité sociale] »[1946].

Par ailleurs, la section « santé » est compétente pour « l'examen des dossiers concernant le traitement de données à caractère personnel relatives à la santé, au sens de la loi du 8 décembre 1992 [...] », à l'exception de ceux qui ressortissent de la compétence de la section sécurité sociale[1947].

Le *Comité sectoriel de la Banque-Carrefour des Entreprises* est compétent pour autoriser « l'accès à d'autres données [de la Banque-Carrefour des Entreprises] »[1948] que celles « qui sont par nature accessibles, sans autorisation préalable »[1949].

Le *Comité sectoriel du Registre national* est compétent pour octroyer « l'autorisation d'accéder aux informations [enregistrées dans le Registre national] »[1950] ainsi que « l'autorisation d'utiliser le numéro d'identification du Registre national »[1951].

Le *Comité de surveillance sectoriel « Phénix »* « contrôle le respect de l'application de la loi du 8 décembre 1992 [...], à la banque de données Phénix »[1952], qui est la banque de données de l'ordre judiciaire.

[1946] Art. 43*bis*, al. 1, de la loi du 15 janvier 1990.

[1947] Art. 43*bis*, al. 2, de la loi du 15 janvier 1990. Voy. également l'art. 42, §2, 3°, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, *M.B.*, 22 décembre 2006. Ainsi, sont soumis à l'autorisation de la section « sécurité sociale » et non à celle de la section « santé », les traitements de données à caractère personnel relatives à la santé, au sens de la loi du 8 décembre 1992, par les institutions de sécurité sociales et les personnes visées à l'art. 18 de la loi du 15 janvier 1990 (art. 15, §2, 2°, et art. 43*bis* de la loi du 15 janvier 1990) ; les traitements de données sociales à caractère personnel relatives à la santé (au sens de la loi du 15 janvier 1990) par les instances d'octroi visées à l'art. 11*bis* de la loi du 15 janvier 1990 (art. 43*bis* de la loi du 15 janvier 1990) et les traitement de données sociales à caractère personnel relatives à la santé par une instance de sécurité sociale vers une autre instance de sécurité sociale, une instance d'octroi visée à l'article 11*bis* de la loi du 15 janvier 1990 ou une personne visée à l'article 18 de la loi du 15 janvier 1990 (art. 15, §1, de la loi du 15 janvier 1990). Sur la question de la compétence d'autorisation de chaque section de ce comité sectoriel, voy. également CPVP, avis n° 43/2006 du 8 novembre 2006 relatif au projet de loi portant dispositions diverses – création d'un comité sectoriel de la sécurité sociale et de la santé, p. 7, n° 15.

[1948] Art. 18, §2 du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, *M.B.*, 5 février 2003. Voy. également l'art. 27 de cette même loi.

[1949] *Ibid.*, art. 17.

[1950] Art. 5 de loi du 8 août 1983 organisant un registre national des personnes physiques. Voy. également l'art. 15 de cette même loi.

[1951] *Ibid.*, art. 8 et 15.

[1952] Art. 22 et s. de la loi du 10 août 2005 instituant le système d'information Phénix, *M.B.*, 1er septembre 2005.

Le *Comité de surveillance Statistique* est compétent pour autoriser l'Institut national de Statistique à « communiquer des données d'étude codées[1953] »[1954].

Enfin, le *Comité sectoriel pour l'Autorité fédérale* a une compétence résiduelle, en ce qu'il est compétent pour autoriser « toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, [...] à moins que la communication n'ait déjà fait l'objet d'une autorisation de principe d'un autre comité sectoriel créé au sein de la Commission pour la protection de la vie privée »[1955].

Comme on l'a dit, la CPVP est soucieuse de ne pas multiplier les comités sectoriels. Dans cette perspective, on s'aperçoit que le Comité sectoriel pour l'Autorité fédérale devient progressivement une autorité « fourre-tout » à qui le législateur attribue la compétence d'autoriser les transferts de données dans des secteurs pour lesquels la nécessité d'instaurer un comité sectoriel spécifique n'est pas établie. C'est la raison pour laquelle les transferts de données par l'intermédiaire de la Banque-Carrefour des véhicules sont du ressort du comité sectoriel pour l'Autorité fédérale et non du comité sectoriel « Mobilité et Transports » qui avait été envisagé[1956].

546.- Le critère de détermination du comité sectoriel compétent. La lecture de ces règles amène à constater que la compétence de chaque comité sectoriel n'est pas toujours définie selon le même critère. Comme on l'a dit précédemment, la compétence de certains comités sectoriels est définie par rapport à la *nature des données contrôlées*. C'est le cas du Comité sectoriel de la Banque-Carrefour des entreprises, du Comité sectoriel du Registre national, du Comité sectoriel Phénix et, en partie du

[1953] Les données d'étude sont « les informations qui serviront à établir des résultats statistiques ». On les dit « codées » lorsqu'elle « ne peuvent être mises en relation avec une personne identifiée que par l'intermédiaire d'un code » [Art. 3 de la loi du 22 mars 2006 « modifiant la loi du 4 juillet 1962 relative à la statistique publique et la loi du 8 août 1983 organisant un Registre national des personnes physiques », *M.B.,* 21 avril 2006. Signalons que cette disposition n'est pas encore entrée en vigueur].

[1954] Art. 17 de la loi du 22 mars 2006 modifiant la loi du 4 juillet 1962 relative à la statistique publique et la loi du 8 août 1983 organisant un Registre national des personnes physiques. Voy. également l'article 35 de cette même loi ainsi que l'arrêté royal du 7 juin 2007 fixant les modalités relatives à la composition et au fonctionnement du Comité de surveillance statistique institué au sein de la CPVP, *M.B.,* 20 juin 2007.

[1955] Art. 36*bis* de la loi du 8 décembre 1992.

[1956] À ce sujet voy. CPVP, avis n° 23/2008, *op. cit.*, n° 73 et s.

moins[1957], du Comité sectoriel sécurité sociale et santé, section « santé ». La compétence d'autres comités sectoriels est définie par rapport à *l'autorité qu'ils contrôlent*. C'est le cas du Comité sectoriel sécurité sociale et santé, section « sécurité sociale » et du Comité sectoriel pour l'Autorité fédérale.

Concrètement, la question du comité sectoriel compétent dans un cas d'espèce peut être résolue en identifiant, tout d'abord, la nature des données réclamées. S'agit-il d'une donnée enregistrée dans la Banque-Carrefour des Entreprises, dans le Registre national, dans la banque de données Phénix ou s'agit-il encore d'une donnée relative à la santé ?

Dans l'affirmative, il y a lieu de s'adresser au comité sectoriel compétent pour contrôler la communication de ces données[1958].

Dans la négative, le comité sectoriel compétent est soit le Comité sectoriel de la sécurité sociale et de la santé, section « sécurité sociale », soit le Comité sectoriel pour l'Autorité fédérale. Si ces deux comités sectoriels sont susceptibles d'intervenir – dans l'hypothèse, par exemple, d'un échange de données entre le SPF Finances et l'ONSS-, il y a lieu d'appliquer le critère de « l'autorité qui communique »[1959], selon lequel le traitement des données réclamées doit être autorisé par « le comité sectoriel compétent vis-à-vis de l'autorité d'où proviennent les données »[1960]. Telle est d'ailleurs la solution dégagée par la CPVP pour répartir les compétences entre les comités sectoriels et ainsi éviter « une compétence concurrente de deux comités sectoriels pour le même flux : celui compétent pour contrôler la communication des données et celui qui le serait pour contrôler la réception »[1961].

[1957] En effet, la communication d'une donnée relative à la santé n'implique pas nécessairement la compétence du comité sectoriel sécurité sociale et santé, section « santé ». Il importe en effet de vérifier qu'une telle communication ne relève pas de la compétence de la section « sécurité sociale ».

[1958] En ce sens, l'art. 45 du Règlement d'ordre intérieur de la CPVP prévoit que « la Commission transmet le dossier au comté sectoriel auquel la compétence dans un domaine déterminé est explicitement attribuée par ou en vertu de la loi » et qu' « entre les comités sectoriels, la règle de l'attribution de la matière par ou en vertu de la loi est en principe applicable ».

[1959] Avis n° 01/2007 du 17 janvier 2007 relatif à un avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances, p. 14, n° 81. Voy. dans le même sens, l'avis n° 01/2005 du 10 janvier 2005 relatif au projet d'arrêté royal organisant l'enregistrement du cancer, p. 6 et l'article 45 du Règlement d'ordre intérieur de la CPVP qui prévoit qu' « en ce qui concerne les dossiers relatifs à des autorisations, le comité sectoriel compétent est celui chargé du contrôle du service public effectuant la communication des données ».

[1960] Avis n° 01/2007, *op. cit.,* p. 14, n° 81.

[1961] Avis n° 01/2005 du 10 janvier 2005, *op. cit.,* p 6.

> Cette solution est consacrée à l'article 45 du Règlement d'ordre intérieur de la CPVP, qui prévoit qu' « en ce qui concerne les dossiers relatifs à des autorisations, le comité sectoriel compétent est celui chargé du contrôle du service public effectuant la communication des données ».

Néanmoins, un conflit de compétence demeure lorsqu'une donnée santé est transmise par une institution de sécurité sociale, telle qu'une mutuelle. Dans ce cas, tant la section santé que la section sécurité sociale sont compétentes. L'article 43 de la loi du 15 janvier 1990 prévoit que, dans ce cas, les deux sections se réunissent pour étudier la demande l'autorisation.

Par conséquent, il n'est pas possible de demander à un comité sectoriel d'avoir accès à des données dont l'autorisation de traitement ne relève pas de sa compétence, fut-ce même par l'intermédiaire d'une plateforme d'échange d'informations.

> La CPVP a rendu un avis à ce sujet, à la demande du Président du Comité sectoriel de la sécurité sociale[1962]. Un organisme ne faisant pas partie du réseau sectoriel de la sécurité sociale avait demandé, au seul Comité sectoriel de la sécurité sociale, l'autorisation d'accéder simultanément aux données du Registre national et des registres de la Banque-Carrefour de la sécurité sociale, et ce, via la Banque-Carrefour de la sécurité sociale et une application intégrée. La CPVP a affirmé « qu'il s'agit d'une problématique qui dépasse le Comité sectoriel de la Sécurité sociale »[1963] et que « lorsque l'accès se fait via un 'intégrateur', il va de soi que celui-ci est tenu de respecter les conditions imposées au bénéficiaire de l'autorisation »[1964]. En d'autres termes, l'utilisation d'une plateforme d'échange d'informations pour acheminer les données réclamées n'est « qu'une modalité d'exécution technique des autorisations concernées »[1965] ; elle ne dispense pas le demandeur des informations d'obtenir une autorisation d'accès auprès de chaque comité sectoriel compétent, fussent-ils plusieurs.

[1962] Avis n° 14/2005 du 28 septembre 2008 faisant suite à une décisions d'évocation dans les dossiers SCSZ/05/70, SCSZ/05/110 et SCSZ/05/113 transmise par le Président du Comité sectoriel de la Sécurité sociale.

[1963] *Ibid.*, n° 10.1.

[1964] *Ibid.*, n° 10.3.

[1965] *Ibid.*, n° 10.4.

C. Le contrôle des traitements de données contestés : la gestion des plaintes, le pouvoir d'enquête, le pouvoir de dénonciation et le pouvoir d'ester en justice

547.- Les traitements de données contestés. La CPVP dispose de certaines prérogatives pour contrôler les traitements de données qui suscitent des contestations. Une déclaration de traitement, la plainte d'un citoyen, un dossier constitué dans le cadre d'une procédure d'avis, une affaire médiatique, sont autant d'occasions qui peuvent convaincre la CPVP de s'intéresser d'un peu plus près à la légalité de certains traitements de données.

La compétence de la CPVP de gérer les plaintes relatives à des traitements de données à caractère personnel a été analysée précédemment[1966]. Outre cette compétence, la CPVP peut enquêter, dénoncer certains traitements au Procureur du Roi et ester en justice[1967].

548.- Le pouvoir d'enquête. Pour s'assurer de la réalité des illégalités commises, la CPVP dispose d'un pouvoir d'investigation. La loi lui octroie ainsi le droit d'exiger la communication de tout document pouvant être utile à l'exercice de ses missions, et celui de pénétrer dans les lieux où sont accomplis des traitements de données[1968].

Cette prérogative est intéressante pour vérifier, notamment, que les responsables de traitements n'utilisent pas des données pour lesquelles ils n'ont pas reçu l'autorisation du comité sectoriel compétent[1969].

549.- La dénonciation au Procureur du Roi. La plupart des obligations imposées par la loi du 8 décembre 1992 sont assorties d'une sanction pénale[1970]. Si ces règles ne sont pas respectées, la CPVP peut dénoncer, au Procureur du Roi, les infractions dont elle aurait connaissance dans l'exercice de ses missions[1971].

[1966] Voy. supra, n° 478.- et s.

[1967] Ces prérogatives sont prévues aux articles 31 et 32 de la loi du 8 décembre 1992. Ils transposent, partiellement du moins, les articles 28.3 et 28.4 de la directive 95/46.

[1968] Art. 32, §1, de la loi du 8 décembre 1992.

[1969] Pour un cas d'utilisation du numéro de Registre national en violation de l'interdiction du Comité sectoriel du registre national, voy. E. Degrave, « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données à caractère personnel illégal sanctionné par la Cour d'appel de Bruxelles », observations sous Bruxelles (9e ch.), 9 mai 2012, J.T., 2012, pp. 691 à 693.

[1970] Art. 38 et 39 de la loi du 8 décembre 1992.

[1971] Voy. l'art. 32, §2, de la loi du 8 décembre 1992.

Néanmoins, il serait inutile de dénoncer au Procureur du Roi les infractions commises par une administration. En effet, les administrations sont des organes de l'État. Or, l'État, bien qu'étant une personne morale de droit public, n'est pas responsable pénalement. En vertu de l'article 5 du Code pénal, l'État et ses organes bénéficient d'une immunité de responsabilité pénale[1972]. La dénonciation d'une administration auprès du Procureur du Roi ne pourrait donc pas mener à une condamnation pénale.

En revanche, si la CPVP avait connaissance de l'identité d'un fonctionnaire qui, au sein d'une administration, effectue des traitements de données illégaux[1973], elle pourrait le dénoncer auprès du Procureur du Roi puisque l'immunité de responsabilité pénale de l'État ne bénéficie pas aux agents de l'administration.

550.- L'action d'intérêt collectif devant le tribunal de première instance. L'article 32, §3, de la loi du 8 décembre 1992 dispose que « [...] le président de la Commission peut soumettre au tribunal de première instance tout litige concernant l'application de la présente loi et de ses mesures d'exécution ». La loi du 8 décembre 1992 reconnaît ainsi à la CPVP un droit d'action collective[1974], celui de saisir le tribunal de première instance pour faire valoir les droits d'un ensemble de citoyens. L'exercice de ce droit initie un contentieux objectif dans le but d'obtenir du juge qu'il mette fin aux pratiques illégales d'un responsable de traitement.

a) Les justifications du droit d'action collective. La CPVP est compétente pour agir dans l'intérêt collectif depuis l'entrée en vigueur de la loi du 8 décembre 1992. Comme en attestent les travaux préparatoires de ladite loi, « c'est précisément parce que les moyens manquent à [la CPVP] de faire respecter ses propres points de vue qu'il est utile de lui permettre d'ester en justice, dans des cas importants, exceptionnels, pour que le juge entérine, par son jugement, le point de vue de la commission et, à

[1972] Sont visés par cette immunité, en vertu de l'article 5 du Code pénal, « l'État fédéral, les Régions, les Communautés, les provinces, les zones de secours, l'agglomération bruxelloise, les communes, les zones pluricommunales, les organes territoriaux intracommunaux, la Commission communautaire française, la Commission communautaire flamande, la Commissuin communautaire commune et les centres publics d'aide sociale ». Cette disposition a été insérée dans le Code pénal par l'article 2 de la loi du 4 mai 1999 instaurant la responsabilité pénale des personnes morales, *M.B.,* 22 juin 1999. À ce sujet, voy. *infra,* n° 593.-

[1973] Sur la possibilité d'identifier le fonctionnaire effectuant des traitements de données illégaux, voy. *supra,* n° 404.-

[1974] Au sujet de l'action d'intérêt collectif, voy. G. DE LEVAL, *Éléments de procédure civile,* Bruxelles, Larcier, 2e éd., 2005, pp. 21 à 23.

ce moment-là, bien entendu, dans le respect des droits de la défense »[1975]. Dès lors, grâce à ce droit d'action, lorsque la CPVP « constate qu'elle se trouve à la limite de ses possibilités, que des recommandations ne suffisent pas [...] elle [peut] faire appel au juge pour qu'il constate qu'un acte donné est contraire à la loi et qu'il prescrive les mesures de contrainte qui s'imposent »[1976].

Une autre justification avancée à l'époque est le fait que le Comité de surveillance de la sécurité sociale[1977] s'était déjà vu reconnaître ce droit d'action[1978]. On a jugé qu'il serait « regrettable que ce comité de surveillance, hiérarchiquement ou fonctionnellement subordonné à la commission, dispose d'un droit que la commission elle-même n'a pas »[1979].

Ce droit d'action est présenté aujourd'hui comme la traduction, en droit belge, du « pouvoir d'ester en justice » de l'autorité de contrôle, visé par la directive 95/46 depuis 1995 et le Protocole additionnel à la Convention n° 108 depuis 2001[1980].

> L'article 1.2 du Protocole additionnel à la Convention n° 108 dispose que « les Parties devraient accorder à l'autorité de contrôle le pouvoir, soit d'ester en justice, soit de porter à la connaissance de la justice toute violation aux principes de la protection des données. Ce pouvoir dérive notamment du pouvoir de mener des investigations qui peuvent conduire l'autorité à constater une violation aux droits des personnes. L'obligation des Parties d'accorder à l'autorité ce pouvoir peut être remplie en lui donnant le pouvoir de prendre des décisions judiciaires ».
>
> L'article 28, §3, alinéa 3, de la directive 95/46 affirme que « chaque autorité de contrôle dispose notamment du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire ».

[1975] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la Commission de la Justice par M. Vandenberghe, *Doc. Parl.,* Ch. Repr., session extr. 1991-1992, n° 445/2, p. 33.

[1976] *Ibid.,* p. 30.

[1977] Il s'agit aujourd'hui du comité sectoriel de la sécurité sociale.

[1978] Il en dispose d'ailleurs toujours, comme en atteste l'article 52 de la loi du 15 janvier 1990 sur la Banque-carrefour de la sécurité sociale.

[1979] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la Commission de la Justice par M. Vandenberghe, *op. cit.,* n° 445/2, p. 30.

[1980] Voy. V. Verbruggen, *Protection des données à caractère personnel (Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)*, Bruxelles, Larcier, coll. Codes commentés Larcier, 2011, p. 228.

b) Le droit d'action collective dans l'e-gouvernement. La compétence de la CPVP d'agir dans l'intérêt collectif est particulièrement intéressante dans l'e-gouvernement.

Tout d'abord, l'exercice de ce droit d'action par la CPVP permet de pallier aux difficultés que rencontrent les citoyens pour contrôler le traitement de leurs données dans l'e-gouvernement. Ainsi qu'on l'a déjà dit, ceux-ci ne sont pas toujours conscients de l'existence de pratiques illégales. De plus, ils risquent de n'avoir ni le courage ni les moyens d'agir pour résoudre un problème dont l'ampleur les dépasse. Il en va d'autant plus ainsi que les voies d'action à leur disposition sont difficiles à mettre en œuvre.

Ensuite, rappelons que les organes de l'État ne sont pas responsables pénalement. Il serait donc sans effet de dénoncer au Procureur du Roi les traitements de données illégaux effectués au sein de l'administration dans l'espoir qu'ils prennent fin. En revanche, en saisissant le tribunal de première instance, la CPVP pourrait demander au juge qu'il ordonne la cessation de ces pratiques illégales. Pour faire pression sur l'administration et la contraindre à respecter la décision judiciaire, la CPVP pourrait demander que cette condamnation soit assortie du paiement d'une astreinte, conformément aux articles 1385*bis* à 1385*nonies* du Code judiciaire.

Enfin, dans l'immédiat, le droit de la CPVP d'agir devant le tribunal de première instance compense le fait que la loi du 8 décembre 1992 ne donne pas à la CPVP le pouvoir de faire cesser les traitements illégaux[1981], ni celui d'imposer des amendes aux responsables de traitements qui ne respectent pas les règles de protection des données[1982].

c) Améliorer l'efficacité de l'action collective. Après avoir discuté avec des membres de la CPVP, il s'avère que cette dernière n'a jamais utilisé ce droit d'agir dans l'intérêt collectif. Elle a néanmoins envisagé très sérieusement de le faire dans l'affaire SWIFT[1983]. Un compromis amiable

---

[1981] Voy. *infra,* n° 551.-

[1982] Voy. *infra,* n° 592.- et s.

[1983] SWIFT est une société établie en Belgique, qui offre à ses clients – des institutions financières – un service de messagerie financière hautement sécurisé. L'infrastructure de SWIFT est constituée de plusieurs bureaux installés dans différents pays, et de deux centres de traitements situés l'un en Europe et l'autre aux États-Unis. Ces centres conservent pendant 124 jours une copie des messages traités par SWIFT, pour répondre aux besoins liés aux éventuelles contestations venant des institutions financières concernées. Suite aux attentats du 11 septembre 2011, l'administration américaine a enjoint à SWIFT de lui transférer des données relatives aux transactions présentant un lien avec le terrorisme. De nombreuses données à caractère personnel ont ainsi été transférées par SWIFT à l'administration américaine, parmi lesquelles certaines étaient protégées par les règles de protection des données européennes, ce qui a suscité de vives critiques de la CPVP notamment. À ce sujet, voy.

a toutefois été trouvé avant que la CPVP saisisse le tribunal de première instance.

Par ailleurs, ce droit d'action serait plus intéressant encore si le législateur en faisait une action en cessation, et accompagnait celle-ci des règles de procédure propres à ce type d'action. En effet, l'action en cessation est un type d'action « comme en référé ». Elle présente plusieurs avantages que n'offre actuellement pas la procédure organisée par l'article 32, §3, de la loi du 8 décembre 1992. Ainsi, l'action en cessation, comme la procédure en référé, permet une décision rapide. Toutefois, à la différence d'une procédure en référé, l'action en cessation ne requiert pas que l'urgence soit prouvée. En outre, elle donne lieu à une décision au fond[1984]. L'action en cessation doit être portée devant le président du tribunal de première instance. Grâce à cette action en cessation, la CPVP pourrait demander au juge de statuer rapidement sur sa demande de faire cesser les traitements de données effectués illégalement.

Pour effectuer cette modification législative, le législateur pourrait s'inspirer de l'action « comme en référé », qui a été prévue à l'article 14 de la loi du 8 décembre 1992, dont il la été question précédemment[1985]. Rappelons que l'article 14 de la loi du 8 décembre 1992 permet d'agir comme en référé pour obtenir du responsable de traitement qu'il respecte certaines obligations limitativement énumérées, à savoir, le droit d'obtenir la communication de données à caractère personnel, et le droit d'obtenir la rectification, la suppression ou l'interdiction d'utiliser des données. Il s'agit donc d'une action qui doit être exercée par les personnes concernées souhaitant obtenir le respect de ces droits.

D'autres institutions bénéficient déjà du droit d'intenter une action en cessation[1986]. Tel est notamment le cas du Centre pour l'égalité des chances et la lutte contre le racisme[1987] que l'on peut utilement comparer à la CPVP en ce que ces deux institutions agissent pour mettre fin à des pratiques illégales portant atteinte à un droit fondamental. En vertu de l'article 20 de la loi du 10 mai 2007, le Centre pour l'égalité des chances peut saisir le président du tribunal de première instance pour qu'il « constate l'existence et ordonne la cessation d'un acte, même pénalement réprimé,

---

not. CPVP, avis n° 37/2006 du 27 septembre 2006 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC) ; Y. POULLET et E. DEGRAVE, « L'affaire SWIFT », *R.D.T.I.,* 2007, pp. 3 à 9.

[1984] C. DALCQ, « Vers et pour une théorie générale du 'comme en référ' : le point sur les questions transversales de compétence et de procédure », *in Les actions en cessation* (dir. J.-F. VAN DROOGHENBROECK), Bruxelles, Larcier, 2006, pp. 60 et 61.

[1985] Voy. *supra,* n° 480.- et s.

[1986] Sur ces institutions, voy. C. DALCQ, *op. cit.,* p. 29.

[1987] Ci-après, « le Centre pour l'égalité des chances ».

constituant un manquement aux dispositions de la présente loi ». Cette action « est formée et instruite selon les formes du référé »[1988].

551.- L'article 28.3 de la directive 95/46. La loi du 8 décembre 1992 ne transpose qu'imparfaitement l'article 28.3 de la directive 95/46 qui énonce les prérogatives des autorités nationales de contrôle.

> Cette disposition prévoit que « chaque autorité de contrôle dispose notamment :
>
> – de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle,
>
> – de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques,
>
> – du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire [...] ».

La CPVP ne dispose ni du pouvoir d'ordonner le verrouillage, l'effacement ou la destruction des données, ni de la possibilité d'interdire temporairement ou définitivement un traitement. Elle n'est pas non plus compétente pour adresser un avertissement ou une admonestation au responsable du traitement. Selon un rapport de l'*European Union Agency for fundamenal rights,* la Belgique est le seul État européen à ne pas conférer de tels pouvoirs à l'autorité nationale chargée de la protection des données[1989]. Ces manquements doivent donc être comblés[1990].

[1988] Loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination, *M.B.,* 30 mai 2007. Au sujet de cette action en cessation, voy. S. VAN DROOGHENBROECK, « L'action en cessation de discriminations », *in Les actions en cessations, op. cit.,* pp. 323 à 397.

[1989] European Union Agency for fundamental rights, Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II, *op. cit.*, p. 23.

[1990] Voy. *infra,* n° 587.-

Section 3. Le contrôle par le détaché à la protection des données

552.- Considérations générales. La directive 95/46[1991] prévoit la possibilité d'instituer un détaché à la protection des données au sein de chaque institution qui traite des données à caractère personnel. Le futur règlement européen en matière de protection des données à caractère personnel en fait même une obligation dans l'administration.

Loin de n'être qu'une formalité administrative supplémentaire, la désignation d'un détaché à la protection des données présente de nombreux avantages pour l'administration. Malheureusement, en Belgique, ce rôle n'a pas encore reçu l'attention qu'il mérite.

I. Le rôle du détaché à la protection des données

553.- La directive 95/46. La directive 95/46 définit le détaché à la protection des données comme la « personne désignée par le responsable du traitement de données [qui] s'assure que les traitements effectués ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées [...] [qui est] employée ou non du responsable du traitement de données, [et] doit être en mesure d'exercer ses fonctions en toute indépendance »[1992].

Pour l'heure, la désignation d'une telle personne est facultative[1993]. Néanmoins, cette situation pourrait se modifier prochainement car, comme on l'a dit, la proposition de règlement européen en matière de

[1991] Considérant 49 et art. 18 de la directive 95/46.

[1992] Considérant 49 de la directive 95/46. Voy. égal. l'art. 18 de la directive 95/46.

[1993] Signalons qu'actuellement, huit États membres de l'Union européenne ont mis en place des détachés à la protection des données, à savoir la France, l'Allemagne, les Pays-Bas, la Suède, le Luxembourg, la Slovaquie, la Hongrie, et l'Estonie. Voy. A. Goyer, *Donne-t-on les moyens au Correspondant informatique et libertés d'être efficace ?*, Rapport de thèse professionnelle, Institut supérieur d'électronique de Paris, Année académique 2008-2009, p. 7 disponible sur le site http://atlas.isep.fr/fccss/images/stories/food/thesesIL/cil%20lui%20donne-t-on%20les%20moyens%20dtre%20efficace_these%20professionnelle_aurli%20goyer_mastre%20informatique%20et%20liberts.pdf ; Sur le cas de la France, de l'Allemagne, des Pays-Bas, de la Suède et du Luxembourg, voy. également Groupe « Article 29 » sur la protection des données, *Rapport sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne*, 18 janvier 2005, WP 106, pp. 16 à 21.

protection des données à caractère personnel rend obligatoire la désignation d'un détaché à la protection des données dans l'administration.

> L'article 35.1 de ladite proposition de règlement dispose que « le responsable du traitement et le sous-traitant désignent systématiquement un délégué à la protection des données lorsque : a) le traitement est effectué par une autorité ou un organisme publics ».

554.- Le détaché à la protection des données en Belgique. Jusqu'à présent, la fonction de détaché à la protection des données a malheureusement fait l'objet de peu d'attention en Belgique.

a) L'absence d'obligation. Le législateur n'impose pas qu'un détaché à la protection des données soit présent dans chaque organisme traitant des données à caractère personnel. Tout au plus, la loi du 8 décembre 1992 cite-t-elle le « préposé à la protection des données »[1994] en guise d'exemple de mesure particulière de protection à l'égard des « traitements présentant des risques particuliers au regard des droits et des libertés des personnes concernées »[1995].

Certes, la loi du 15 janvier 1990 prévoit l'obligation, pour toute institution de sécurité sociale, de désigner un « conseiller en sécurité ». Néanmoins, ce rôle n'est pas à confondre avec celui de détaché à la protection des données. Comme l'affirme la CPVP, la notion de détaché à la protection des données « indique, en effet, que la mission de cette personne est plus large que celle de veiller à la sécurité des données, y compris l'intégrité et la disponibilité mais comprend aussi le devoir 'd'assurer, d'une manière indépendante, l'application de la [loi du 8 décembre 1992] ainsi que de ses mesures d'exécution', ce qui signifie outre les missions de

[1994] Dans un souci de clarté, la section de législation du Conseil d'État avait recommandé de reprendre, dans la loi belge, les termes « détaché à la protection des données », utilisé par la directive 95/46. [voy. SLCE, avis du 2 février 1998 sur un avant-projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *op. cit.,* sess. 1997-1998, n° 1566/1, p. 233].Cela n'a pourtant pas été fait. Quoi qu'il en soit, les notions de « détaché à la protection des données » et de « préposé à la protection des données » désignent la même fonction.

[1995] Art. 17*bis,* de la loi du 8 décembre 1992. Pour un cas d'application de cette disposition, voy. CPVP, avis n° 27/2007 du 4 juillet 2007 sur un projet d'arrêté royal précisant les règles relatives au traitement des listes négatives.

sécurité, celle du contrôle du respect des principes de légitimité, de proportionnalité et du droit d'accès des personnes concernées »[1996].

> En n'organisant pas d'obligation de recourir à un détaché à la protection des données, la Belgique se distingue de l'*Allemagne*, qui rend obligatoire la présence d'un détaché à la protection des données dans les organismes du secteur public, au niveau fédéral et dans certains états[1997].
>
> La Belgique se distingue également de la *Suisse*, qui impose un détaché à la protection des données dans les institutions fédérales[1998].
>
> Cette obligation existe également en dehors des frontières européennes. Ainsi, au *Québec*, il y a, dans chaque organisme public, une « personne responsable de la protection des renseignements personnels »[1999], chargée notamment de tenir le registre toutes les communications de renseignements effectuées par l'organisme émetteur[2000], d'organiser les ententes de partage avec les autres administrations[2001], etc. Ce responsable est « la personne ayant la plus haute autorité au sein [de l'] organisme public »[2002]. Celle-ci peut toutefois « désigner comme responsable un membre de l'organisme public ou de son conseil d'administration [...] ou un membre de son personnel de direction » à qui il peut « déléguer tout ou partie de ses fonctions »[2003].

b) L'absence de statut. Plus encore, ni le législateur ni le Roi n'ont défini le statut du détaché à la protection des données. La loi du 8 décembre 1992 se contente de renvoyer au Roi le soin de déterminer le statut du détaché à la protection des données, ce qui n'a jamais été fait. Dès lors,

---

[1996] CPVP, avis n° 19/2002 du 10 juin 2002 relatif à un projet de la loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, à un Projet d'arrêté royal relatif aux cartes d'identité, à un projet d'arrêté royal portant mesures transitoires en ce qui concerne la carte d'identité électronique en Belgique, p. 11, n° 22.

[1997] Art. 4f (1) de la *Bundesdatenschutzgesetz*. Pour un commentaire de ce régime, voy. N. Métallinos, « La fonction de 'détaché à la protection des données' en Allemagne et aux Pays-bas », *Droit social,* n° 12, 2004, p. 1068.

[1998] Art. 23 de l'Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993.

[1999] Art. 8 de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.

[2000] Art. 67.3 de la loi de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.

[2001] Art. 64 de la loi de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.

[2002] Art. 8 de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.

[2003] *Idem*.

aucune garantie n'est établie pour assurer l'indépendance du détaché à la protection des données.

Cette lacune suscite des critiques de la part de la section de législation du Conseil d'État, qui insiste sur la nécessité que le législateur fixe le statut des détaché à la protection des données « en vue de garantir au mieux leur indépendance, parce qu'on ne peut totalement exclure que leur situation, notamment leur appartenance aux institutions où les traitements ont lieu, ne mette cette indépendance en péril »[2004]. Il s'agit là d'un point qui doit être réglé par le pouvoir législatif, et non le pouvoir exécutif, en vertu de l'article 22, alinéa 2 de la Constitution et du principe de légalité y consacré[2005]. La section de législation du Conseil d'État affirme que si « le législateur n'[est] pas en mesure de déterminer, dès à présent, dans l'avant-projet de loi, quelles seront les garanties de cette indépendance effective, par l'énoncé de règles précises, le concept [...] doit être abandonné ; en effet, confier au Roi, comme le fait très indirectement le projet, le soin de régler la matière, ne se conçoit pas, en raison de l'article 22, alinéa 2, de la Constitution, et parce qu'il serait anormal que le pouvoir exécutif trace les contours de cette indépendance, alors qu'il n'est pas exclu que celui-ci désigne en son sein des délégués, en sa qualité de responsable de nombreux traitements visés par la loi »[2006].

La CPVP critique également l'absence de statut légal du détaché à la protection des données[2007]. Elle tente néanmoins de pallier ce silence en apportant quelque éclairage à ce sujet. Elle livre des critères pour garantir effectivement cette indépendance, faisant écho à des législations étrangères.

[2004] SLCE, avis du 2 février 1998 sur un avant-projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *op. cit.,* sess. 1997-1998, n° 1566/1, p. 232.

[2005] À ce sujet, voy. *supra,* Titre I. La légalité de l'e-gouvernement.

[2006] SLCE, avis du 2 février 1998 sur un avant-projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *op. cit.,* sess. 1997-1998, n° 1566/1, p. 232.

[2007] CPVP, avis n° 15/2002 du 2 mai 2002 relatif à un projet d'arrêté royal portant exécution de l'article 3, §6, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, n° 17 ; CPVP, avis n° 35/2012 du 21 novembre 2012 sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, n° 128.

La CPVP affirme ainsi que l'indépendance du détaché à la protection des données signifie notamment qu'il doit pouvoir initier des projets ou en refuser, *sans pression extérieure*[2008].

En outre, l'exercice des missions confiées au détaché à la protection des données ne peut lui causer des *désavantages*, tel qu'un licenciement ou une réaffectation à un autre poste[2009]. C'est particulièrement important lorsque la législation prévoit la possibilité, pour le détaché à la protection des données, d'alerter l'autorité nationale de contrôle en matière de protection des données d'une pratique illégale au sein de son institution, comme c'est le cas en France[2010]. En d'autres termes, le détaché à la protection des données ne doit pas craindre un licenciement s'il est contraint de dénoncer des pratiques illégales au sein de l'institution qui l'a engagé. Or, la peur d'entrer en conflit avec la direction de l'institution pourrait mettre en cause l'indépendance du détaché à la protection des données. Il semble donc nécessaire que cette personne jouisse d'un statut de salarié protégé, comme c'est le cas en Allemagne où les détachés à la protection des données ne peuvent être licenciés par l'employeur que pour des raisons importantes[2011].

Enfin, pour garantir cette indépendance, la CPVP conseille de placer le détaché à la protection des données à un *niveau de hiérarchie* « tel qu'il ait la possibilité de communiquer directement avec le management/comité

[2008] Voy. not. CPVP, avis n° 39/2008 relatif au projet d'arrêté royal relatif à l'accès des personnes désignées de l'Office des Etrangers aux faits concrets de police judiciaire et aux informations relatives aux groupements et aux personnes traitées dans le cadre des missions de police administrative et centralisée dans la banque de données Nationale générale, visée à l'article 44/4 de la loi du 5 août 1992 sur la fonction de police, n° 31.

[2009] *Idem*.

[2010] L'article 51 du décret du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que « la Commission nationale de l'informatique et des libertés peut être saisie à tout moment par le correspondant à la protection des données à caractère personnel ou le responsable des traitements de toute difficulté rencontrée à l'occasion de l'exercice des missions du correspondant. L'auteur de la saisine doit justifier qu'il en a préalablement informé, selon le cas, le correspondant ou le responsable des traitements.

La Commission nationale de l'informatique et des libertés peut à tout moment solliciter les observations du correspondant à la protection des données ou celles du responsable des traitements ».

[2011] L'article 4f, § 3, de la *Bundesdatenschutzgesetz* prévoit que la nomination au poste de détaché à la protection des données peut être annulée en application du § 626 du *Bürgerliches Gesetzbuch* (Code civil allemand) qui prévoit que des raisons importantes doivent être établies pour mettre fin au contrat ; C. KLUG, « Improving self-regulation trough (law-based) Corporate Data protection Officials », disponible sur le site de l'association des détachés à la protection des données allemands, www.gdd.de.

de direction et d'exercer sa mission directement auprès du responsable de traitement »[2012].

II. L'intérêt d'instituer un détaché à la protection des données dans chaque administration

555.- Une fonction importante. Même si le législateur belge n'a pas saisi la possibilité offerte par la directive 95/46 d'instituer des détachés à la protection des données dans chaque administration, cette fonction ne peut pour autant être sous-estimée. Puisque dans quelques années, suite à l'entrée en vigueur du nouveau règlement européen sur la protection des données, chaque administration sera obligée de disposer de son propre détaché à la protection des données, il importe, dès aujourd'hui, de s'interroger sur les compétences et les missions des personnes qui seront affectées à ce rôle. Au-delà même de la mise en œuvre de cette obligation future, on doit saisir pleinement l'intérêt, dans l'immédiat, d'instituer des détachés à la protection des données dans l'administration, tant au regard de la protection des données à caractère personnel que par rapport au souci légitime des administrations de minimiser les formalités qui alourdissent leur travail quotidien.

A. L'amélioration de la protection des données à caractère personnel

556.- Veiller à la légalité et de la transparence des traitements. Comme dit précédemment, la mission du détaché à la protection des données est définie de manière large par la directive 95/46 puisqu'il revient à cette personne de s'assurer « que les traitements effectués ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées »[2013]. Par ce rôle ample, le détaché à la protection des données peut être appelé à se prononcer sur tous les aspects des traitements de données mis en place dans l'administration, tant en ce qui concerne leur légalité que leur transparence.

> C'est d'ailleurs en ce sens que s'est prononcée la section de législation du Conseil d'État pour insister sur l'importance de définir le statut du détaché à la protection des données. Selon la haute juridiction, « la loi en projet charge le préposé de 'contrôler' l'application de la loi ; la directive, dans son texte français, lui prescrit d' 'assurer' celle-ci ; cette expression, pour ce

[2012] *Idem.*

[2013] Considérant 49 de la directive 95/46.

> qu'elle implique de pouvoir d'initiative, d'autonomie et de responsabilité, doit être préférée à celle de l'avant-projet, et inspirer le législateur dans sa détermination du statut des détachés, au nom de l'efficacité de ce contrôle décentralisé »[2014].

Cette personne peut donc œuvrer substantiellement à l'amélioration de la protection de la vie privée au sein de l'organisme qui l'engage. Elle peut le faire d'autant mieux qu'elle maîtrise, en principe, tant la matière de la protection des données à caractère personnel, que les particularités de l'organisme au sein duquel elle travaille[2015]. Sa mission s'assimile à un mécanisme d'autorégulation qui pourrait compenser certaines faiblesses du système de protection actuel. Dans son rapport sur le rôle des détachés à la protection des données, le Groupe européen dénommé « Article 29 » sur la protection des données, fait même état du fait qu'en Allemagne, « de l'avis général, c'est essentiellement aux détachés à la protection de la vie privée que l'on doit le succès de la protection des données. Une nouvelle profession a été créée, avec sa propre formation et d'importantes activités d'échange d'information sous la forme de congrès, de séminaires, de périodiques et d'autres publications ». D'ailleurs, « le secteur allemand de la protection des données a prouvé son efficacité lors de la consultation de la Commission sir la mise en œuvre de la directive. Près de 50 % de toutes les réponses fournies venaient d'Allemagne »[2016].

On a ainsi souligné à plusieurs occasions que la CPVP n'est pas en mesure de veiller à la protection de la vie privée dans toutes les administrations. Les illégalités commises dans une administration sont d'ailleurs difficiles à percevoir de l'extérieur. Il existe, certes, l'obligation de déclaration. Néanmoins, cette obligation est assortie de nombreuses exceptions en faveur de l'administration. En outre, quand elle est obligatoire, elle n'est pas nécessairement très utile. On conçoit aisément que le responsable de traitement ne déclare pas les traitements illégaux. Quand bien même de tels traitements seraient déclarés, la CPVP n'a pas les moyens de les étudier tous minutieusement et de sanctionner l'entièreté des illégalités commises. Le contrôle de la CPVP se concentre donc principalement sur les traitements

[2014] SLCE, avis du 2 février 1998 sur un avant-projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *op. cit.,* sess. 1997-1998, n° 1566/1, p. 234.

[2015] Sur les connaissances et les qualités exigées d'un détaché à la protection des données, voy. N. Métallinos, *op. cit.,* pp. 1069 à 1071 ; A. Goyer, *op. cit.,* p. 10.

[2016] Groupe « Article 29 » sur la protection des données, Rapport sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne, *op. cit.*, p. 19.

de données ayant fait l'objet d'une plainte ou d'une dénonciation dans la presse, qui ne constituent qu'une minorité des traitements effectués.

§1. Le détaché à la protection des données et la légalité des traitements de données

557.- Un rôle à plusieurs facettes. Le détaché à la protection des données peut se voir confier de multiples tâches en lien avec la légalité des traitements de données à caractère personnel, telles que l'encadrement des fonctionnaires appelés à utiliser les outils informatiques, le contrôle de la collecte et de l'échange des données ainsi que le maintien d'un contact avec la CPVP.

558.- L'encadrement des fonctionnaires. Une fois l'outil de traitement de données organisé par le législateur et le pouvoir exécutif, il est mis en état de fonctionnement au sein de l'administration concernée. Il importe alors de veiller à la légalité de son utilisation, rôle qui pourrait être assuré par le détaché à la protection des données. Le détaché à la protection des données pourrait ainsi assurer l'information et la formation des fonctionnaires appelés à utiliser l'outil informatique.

> Prenons l'exemple d'une administration intégrée dans un réseau sectoriel et appelée à participer à l'échange d'informations au sein de ce réseau. Il serait utile, pour les fonctionnaires de cette administration, de recevoir des explications sur ce réseau sectoriel et la plateforme d'échanges d'informations mise en place, ainsi que sur le rôle joué par leur administration dans ce modèle nouveau. Il importerait également d'attirer leur attention sur leurs obligations en termes de protection des données à caractère personnel en insistant notamment sur le respect des exigences de finalité et de proportionnalité du traitement et des données. Ces tâches devraient pouvoir être accomplies par le détaché à la protection des données. Par ailleurs, cette personne pourrait également disposer d'un accès aux logs, de manière à détecter les éventuelles utilisations abusives de données au sein de l'institution.
>
> En ce sens, la loi fédérale allemande prévoit que le « délégué à la protection des données » est chargé de « 1. surveiller l'utilisation conforme des logiciels de traitement de données grâce auxquels les données personnelles doivent être traitées ; à cet effet, il doit être informé en temps utile des projets de traitement automatisé de données personnelles. 2. familiariser par le biais de mesures appropriées les personnes employées au traitement de données personnelles avec les dispositions de la présente loi et autres dispositions relatives à la protection des données, ainsi qu'avec les exigences particulières respectives concernant la protection des données »[2017].

[2017] Art. 4g de la *Bundesdatenschutzgesetz*

559.- La collecte et l'échange des données. Le détaché à la protection des données pourrait également se voir confier le soin de veiller à la légalité de la collecte des données et des échanges d'informations avec d'autres administrations, car il pourrait être impliqué dans la conclusion d'ententes de partage[2018].

560.- Le dialogue avec la CPVP. Le détaché à la protection pourrait également être un interlocuteur privilégié de la CPVP, afin, notamment, de lui faire état des difficultés juridiques soulevées par les traitements de données menés au sein de son institution et d'être tenu au courant de ses recommandations en la matière.

§2. Le détaché à la protection des données et la transparence des traitements de données

561.- Considérations générales. La présente recherche a déjà abondamment souligné l'importance, mais également la difficulté, d'assurer la transparence des traitements de données à caractère personnel à l'égard des personnes concernées par ceux-ci. Le détaché à la protection des données pourrait également accomplir des tâches essentielles à cet égard, telles que la constitution d'inventaires de données et le suivi des citoyens.

562.- La constitution d'inventaires de données. Comme l'a affirmé le Titre II[2019], chaque administration responsable d'une source authentique des données devrait pouvoir donner aisément accès aux types de données contenus dans la source authentique. Cette tâche pourrait être dévolue au détaché à la protection des données, qui serait également chargé de mettre à jour l'inventaire des données.

> En ce sens, au Québec, il revient notamment au « responsable de la protection des renseignements personnels », d' « établir et de maintenir à jour un inventaire [des fichiers de renseignements personnels » de l'organisme public au sein duquel il travaille[2020].
>
> En Suisse, le « registre des fichiers » est géré par le « préposé » et est « accessible en ligne au public. Sur demande, le préposé communique gratuitement des extraits du registre »[2021].

[2018] Voy. *supra,* n° 222.- et s. Voy. égal. *infra,* n° 599.- et s.

[2019] Voy. *supra,* n° 391.-

[2020] Art. 8 et 76 de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.

[2021] Art. 28 de l'Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993.

563.- Le point de contact des citoyens. Le détaché à la protection des données peut également assurer le rôle de point de contact pour les citoyens désireux de poser des questions relatives à la protection de leur vie privée.

B. L'allègement des formalités administratives

564.- Une dispense de l'obligation de notification des traitements. La désignation d'un détaché à la protection des données permet également d'alléger les formalités auxquelles sont actuellement soumises les administrations. En effet, ainsi qu'on l'a dit dans le Titre II[2022], tout responsable de traitement doit, en principe, notifier chaque traitement de données à l'autorité de protection des données. C'est ce que prévoit l'article 18 de la directive 95/46, relative à la « notification ». Cette obligation a été transposée, dans la loi du 8 décembre 1992, par l'article 17, qui concerne la « déclaration » des traitements de données à caractère personnel.

Cependant, la directive 95/46 prévoit une dispense à cette obligation de notifier les traitements de données, dans l'hypothèse où un détaché à la protection des données a été désigné, et à la condition que ce dernier tienne un registre des traitements effectués par le responsable du traitement.

> Ainsi, l'article 18, §2, de la directive 95/46 prévoit que les États membres ne peuvent prévoir de simplification de la notification ou de dérogation à cette obligation que dans les cas et aux conditions suivantes :
>
> – [...]
>
> – lorsque le responsable du traitement désigne, conformément au droit national auquel il est soumis, un détaché à la protection des données à caractère personnel chargé notamment d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive, de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'article 21, §2[2023], et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées.

a) Une incitation à désigner un détaché à la protection des données. En prévoyant une dispense à l'obligation de notification, la directive 95/46 offre aux responsables de traitements une « victoire contre la

[2022] Voy. *supra,* n° 366.- et s.

[2023] Il s'agit des informations figurant dans le registre des traitements détenu par l'autorité nationale de contrôle. En Belgique, il s'agit du registre public tenu par la CPVP.

bureaucratie »[2024], qui doit les inciter à désigner un détaché à la protection des données. En effet, la notification des traitements de données à l'autorité de protection des données est une formalité lourde pour les responsables de traitements. Bien souvent, de nombreux traitements de données doivent être déclarés. Pour chacun de ceux-ci, des précisions multiples doivent être fournies à l'autorité de protection des données. En outre, cette formalité peut avoir un coût.

En Belgique, cette formalité est coûteuse. Le montant de la contribution à payer à la CPVP pour chaque déclaration de traitement est de 125 euros si la déclaration est présentée sur un formulaire papier, et de 25 euros si elle est présentée sur un support magnétique. La déclaration d'une ou plusieurs modifications apportées aux mentions de la déclaration originale coûte 20 euros[2025].

b) Une dispense non applicable en Belgique. Malheureusement, jusqu'à présent, le législateur belge ne semble pas avoir pleinement saisi l'intérêt de cette possibilité offerte par la directive. N'ayant pas organisé le statut des détachés à la protection des données ni leur mode de désignation, cette dispense de déclaration n'est pas offerte aux responsables de traitement belges.

Néanmoins, certains parlementaires se sont saisis de cette question[2026] et proposent une modification de la loi du 8 décembre 1992 consistant à remplacer l'obligation de déclaration par l'institution de détachés à la protection des données auprès de chaque responsable de traitement. Cette proposition est intéressante, à la condition de ne pas entraîner un recul dans la transparence des traitements de données. Il conviendrait alors d'organiser minutieusement les obligations du détaché à la protection des données en matière de transparence notamment. Cette proposition de loi

[2024] Rapport sur les détachés à la protection des données (DPOs) désignés par les responsables de traitement en application de l'article 18 § 2 de la Directive 95/46/EC présenté par A. Turk à la conférence européenne des Commissaires à la protection des données de Cracovie des 25 et 26 avril 2005, p. 10, disponible sur le site http://www.giodo.gov.pl/data/filemanager_pl/663.pdf

[2025] Art. 47 à 49 de l'arrêt royal du 13 février 2001.

[2026] Proposition de loi du 26 mai 2011 modifiant la oi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitement de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information, *Doc. Parl.,* Ch. Repr., sess. 2010-2011, n° 53-1509/001.

du 26 mai 2011 est motivée par le constat que les objectifs de la déclaration de traitement ne sont pas atteints dans la pratique[2027].

> « Le premier objectif du législateur était non pas de créer des formalités administratives supplémentaires, mais de sensibiliser les intéressés aux aspects liés à la protection de la vie privée et aux conséquences possibles. Dans les faits, il s'avère que l'effet éducatif et sensibilisateur de ces formalités est très limité chez les intéressés. Un deuxième objectif du législateur consistait à permettre à chaque Belge d'obtenir, par l'intermédiaire de cette banque de déclarations centrale, des informations sur le traitement de ses données à caractère personnel, grâce à un registre renseignant qui traitait les données à caractère personnel et où il le faisait. À l'époque, un nombre limité de grosses machines *'mainframe'* effectuaient un traitement automatisé. Depuis lors, les TIC ont connu un essor considérable »[2028]. Partant de ce constat, la proposition de loi prévoit que « l'obligation de déclaration est supprimée. Le responsable du traitement doit désigner dorénavant un conseiller en sécurité[2029] de l'information. Celui-ci est chargé de conseiller, d'encourager, de documenter et de contrôler. [...] L'organisation concernée est libre de désigner un de ses collaborateurs ou un conseiller externe pour accomplir cette mission »[2030].

*

Conclusions

Le régime juridique de la protection des données à caractère personnel organise des voies de contrôle originales, adaptées aux particularités du secteur des traitements de données à caractère personnel. Ces moyens

[2027] Ce même constat a convaincu l'Allemagne de mettre en place des détachés à la protection des données et de supprimer le registre public. Voy. Groupe « Article 29 » sur la protection des données, *Rapport sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne*, *op. cit.*, pp. 17 à 19.

[2028] Proposition de loi du 26 mai 2011 modifiant la oi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitement de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information, *op. cit.*, n° 53-1509/001, p. 5.

[2029] À notre sens, l'utilisation des termes « conseiller en sécurité » est maladroite. Elle vise le rôle consacré par la loi sur la Banque-Carrefour de la sécurité sociale qui impose la présence d'une personne chargée de veiller à la sécurité des systèmes informatiques dans chaque institution de sécurité sociale. Il semble pourtant qu'en l'occurrence, le législateur vise plutôt le rôle de détaché à la protection des données.

[2030] Proposition de loi du 26 mai 2011 modifiant la oi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitement de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information, *op. cit.*, n° 53-1509/001, p. 9.

d'action sont rapides, et ne s'encombrent pas de procédures lourdes. En outre, ils favorisent l'action et la responsabilisation des acteurs principaux de l'e-gouvernement. Ainsi, les citoyens peuvent exercer certains droits auprès de l'administration qui traite leurs données. Ils disposent également d'actions judiciaires particulières. En outre, au sein de chaque administration, un agent spécialisé dans les règles de protection des données peut assurer la fonction de détaché à la protection des données. Enfin, la CPVP est une autorité de régulation spécifiquement vouée au contrôle des traitements de données à caractère personnel.

Néanmoins, ces contrôles manifestent des faiblesses dans le contexte de l'e-gouvernement. La difficulté, pour un individu dont les données sont traitées, d'exercer les droits qui sont les siens accentue le déséquilibre, déjà dénoncé, entre les citoyens et l'administration. Le statut de détaché à la protection des données n'est pas encore organisé en Belgique, si bien que ce rôle est méconnu et trop peu utilisé dans l'administration belge. C'est pourquoi, dans ce chapitre, nous avons proposé des solutions susceptibles d'endiguer ces difficultés.

Enfin, la CPVP a retenu toute notre attention. Dans un premier temps, son statut a été étudié. La CPVP est, en effet, soumise à une exigence d'indépendance, imposée par les règles supranationales et nationales de protection des données et interprétée largement par le Cour de justice de l'Union européenne. Néanmoins, en pratique, il n'est pas certain que la CPVP respecte pleinement cette exigence. En outre, la légitimité de notre autorité de protection des données soulève également des questions relatives au contrôle politique de cette autorité. On a ainsi analysé la tension qui existe entre la jurisprudence de la Cour de justice de l'Union européenne et celle de la Cour constitutionnelle. On s'est également interrogé sur le contrôle juridictionnel de la CPVP et la qualité d'autorité administrative de cette institution.

Dans un deuxième temps, les moyens d'action de la CPVP ont été analysés. Certains de ces moyens se rapprochent des moyens d'action juridiques classiques. D'autres sont empreints de davantage de souplesse. La CPVP peut ainsi contrôler les traitements de données en projet et en cours d'exécution, ainsi que les traitements de données contestés. Néanmoins, il est apparu que ces moyens d'action manquent actuellement d'efficacité.

C'est au départ de ces failles que s'écrit à présent le troisième chapitre.

*

CHAPITRE III.
L'organisation d'un e-gouvernement contrôlé

565.- Introduction. Le premier chapitre a montré la pertinence des contrôles traditionnels de droit administratif pour protéger la vie privée des citoyens. Bien que ces moyens d'action aient été organisés avant l'ère informatique et en dehors des préoccupations de protection des données, ils s'avèrent utiles pour encadrer efficacement l'e-gouvernement, notamment grâce aux sanctions draconiennes qu'ils organisent.

Néanmoins, bien que pertinents, ces contrôles sont insuffisants pour garantir à eux seuls la protection de la vie privée dans l'e-gouvernement, principalement parce que les citoyens n'usent pas des voies de recours traditionnelles à leur disposition. Bien souvent, ils n'ont pas connaissance du traitement de leurs données dans l'administration et ignorent leurs droits en la matière. Quand bien même ils seraient conscients des illégalités commises, ils n'ont probablement pas le courage ni les moyens de faire valoir leurs droits face à un problème d'une ampleur qui les dépasse largement. Par ailleurs, la richesse des règles de protection des données ne reçoit pas toujours l'attention qu'elle mérite lors du contrôle politique et du contrôle juridique de l'e-gouvernement. On peut espérer que ce ne soit qu'une question de temps, et que la situation puisse être améliorée en faisant connaître davantage cette matière dans les cours universitaires, les cénacles parlementaires, les formations d'agents de l'administration, d'avocats et de magistrats, de manière à ce que les violations du régime juridique de la protection des données soient plus régulièrement dénoncées et sanctionnées.

Dans ce contexte, la CPVP joue un rôle essentiel pour veiller à la protection des données. Elle régule le secteur des traitements de données à caractère personnel, et complète ainsi l'action du législateur et du gouvernement en ce domaine. Ainsi qu'on l'a dit, l'existence une autorité spécifiquement vouée à la protection des données est justifiée principalement par l'expertise de ses membres, par l'indépendance de son action, et par l'efficacité de ses contrôles. L'expertise des membres de la CPVP est imposée par la loi du 8 décembre 1992 et ne suscite pas de critique particulière. En revanche, l'efficacité de la CPVP devrait être renforcée. Il en va de même de l'indépendance de notre autorité de protection des données, étroitement liée à la légitimité de celle-ci.

Dès lors, les propos qui suivent plaident pour un renforcement de l'indépendance et de la légitimité de notre autorité de protection des données, ainsi qu'un renforcement de son efficacité.

*

Section 1. Le renforcement de l'indépendance et de la légitimité de la CPVP

566.- Une tension inhérente. Le statut de l'autorité de protection des données pose la question de sa légitimité : la CPVP peut-elle valablement agir dans notre société démocratique compte tenu du fait qu'elle est indépendante ? Comment dépasser ce qui apparaît à première vue comme une contradiction, et définir le statut d'une autorité qui soit tout à la fois protégée de toute pression extérieure, comme l'exige le droit européen, et suffisamment soumise à un contrôle démocratique, comme l'impose notre système constitutionnel ?

Nombre d'États sont confrontés à cette même question au moment d'organiser le statut de leur autorité de protection des données.

> Par exemple, l'Allemagne et l'Autriche, qui croyaient pourtant s'être conformées aux exigences européennes, sont contraintes de remettre l'ouvrage sur le métier, suite aux arrêts de la Cour de justice de l'Union européenne de mars 2010 et d'octobre 2012.
>
> En France, la création de la Commission nationale de l'informatique et des libertés (« CNIL ») a généré la création d'un modèle nouveau d'autorité, celui de l'autorité administrative indépendante.
>
> Au-delà des frontières européennes, la question suscite également nombre de réflexion, comme en témoignent les exemples canadien et québecquois sur lesquels nous reviendrons dans la suite de ces lignes.

Bien que cet exercice soit périlleux, des solutions peuvent être proposées. Elles supposent que des modifications soient apportées au statut de la CPVP, en vue de parfaire son indépendance et sa légitimité.

I. Le renforcement de l'indépendance de la CPVP

567.- Indépendance des membres et indépendance de l'institution. L'indépendance de la CPVP tient surtout à l'indépendance de ses membres, puisque ce sont eux qui délibèrent et prennent les décisions. Pour autant, le statut institutionnel de la CPVP n'est pas à négliger.

A. L'indépendance des membres de la CPVP

568.- Un ou plusieurs commissaires ? Pour l'heure, la CPVP est un organe collégial, comme l'est, par exemple, la CNIL en France[2031]. Comme on l'a dit, le souci du pluralisme et de l'expertise préside à ce type d'organisation. En outre, la collégialité est également présentée comme un gage d'indépendance. L'anonymat engendré par la collégialité réduirait le risque que les membres de l'autorité soient soumis à des pressions extérieures[2032]. Néanmoins, en Belgique, la composition actuelle de la CPVP, bien que collégiale, ne permet pas d'atteindre à suffisance l'objectif d'indépendance. Le problème du « contrôleur-contrôlé » est favorisé, en raison du fait que la loi du 8 décembre 1992 n'empêche pas que le fonctionnaire d'une administration soumise au contrôle de la CPVP soit également membre de cette institution. Ce problème s'étend même aux comités sectoriels étant donné qu'un membre de la CPVP peut également être membre d'un ou plusieurs comités sectoriels.

Dès lors, la question mérite d'être posée de savoir comment composer la CPVP de manière à en garantir l'indépendance. Deux solutions se dégagent.

a) Plusieurs commissaires et des incompatibilités. Une première solution est de maintenir une composition collégiale à la condition de renforcer l'indépendance de chaque membre désigné. À cet égard, la solution française est intéressante.

> En France, l'objectivité et l'impartialité de la CNIL est organisée au travers d'une composition pluraliste qui vise à concilier les intérêts de personnes venant d'horizons distincts. Ainsi, la CNIL comprend quatre parlementaires (deux députés, deux sénateurs), six hauts magistrats (deux conseillers d'État, deux conseillers à la Cour de cassation et deux conseillers à la Cour des comptes), ainsi que deux membres du Conseil économique, social et environnemental. Ces douze membres sont élus par l'assemblée ou la juridiction dont ils émanent. S'ajoutent à ces membres cinq personnalités qualifiées, dont une est désignée par le Président de l'Assemblée nationale, une par le Président du Sénat et trois par décret.

[2031] La CPVP comprend 16 membres tandis que la CNIL en compte 17. D'autres autorités de protection des données sont également collégiales mais comprennent un nombre inférieur de membres. C'est le cas de la Commission nationale de la protection des données du Luxembourg, qui comprend trois membres.

[2032] Dans le même sens, Office parlementaire d'évaluation de la législation (France), *Rapport sur les autorités administratives indépendantes,* Sénat, session 2005-2006, n° 404, p. 73.

En outre, des incompatibilités de mandats devraient être prévues par la loi. Ainsi serait-il préférable d'instaurer une incompatibilité entre l'exercice d'un mandat de membre de la CPVP et/ou d'un comité sectoriel, et un poste de directeur d'une administration.

b) Un commissaire. Une autre solution serait de désigner une personne qui présente elle-même suffisamment de garanties d'expertise, d'objectivité et d'impartialité dans ce domaine, sans exclure qu'elle puisse s'entourer d'une équipe de conseillers. Cette personne serait élue par le Parlement, au terme d'un examen et d'une audition. Elle incarnerait la protection de la vie privée face à l'opinion publique. Plusieurs autorités de protection des données sont organisées de cette manière.

> Tel est le cas, notamment, en Suisse, en Allemagne et au Canada.
>
> En Suisse, les missions de l'autorité de protection des données sont exercées par le Préposé fédéral à la protection des données et à la transparence[2033]. Ce dernier est rattaché administrativement à la Chancellerie fédérale. Il est aidé par un secrétariat permanent ainsi que trois unités regroupant plusieurs personnes. Deux de ces unités sont compétentes pour des questions de protection des données tandis que la troisième se charge de la transparence.
>
> En Allemagne, le *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit* est nommé par le Gouvernement fédéral pour une durée de cinq ans renouvelable une fois[2034]. Comme le Préposé fédéral à la protection des données et à la transparence en Suisse, le Commissaire à la protection des données allemand est entouré d'une équipe structurée en différents départements en fonction des matières traitées[2035].
>
> Le Commissariat à la protection de la vie privée du Canada est également organisé de cette manière. Il est composé d'une Commissaire, qui a la qualité de haute fonctionnaire du Parlement[2036]. Elle est entourée d'une Commissaire adjointe[2037] et d'un Comité consultatif externe[2038] composé d'une vingtaine de personnes spécialisées dans la protection de la vie privée et issues de différents milieux (universités, entreprises privées, administrations, magistrature, etc.).

[2033] Art. 26 et s. de la Loi fédérale sur la protection des données du 19 juin 1992.

[2034] B*undesdatenschutzgesetz*, §22.

[2035] http://www.bfdi.bund.de/EN/FederalDataProtectionCommissioner/StructureAndTasks/organisation_node.html

[2036] Sur la Commissaire à la protection de la vie privée du Canada, voy. http://www.priv.gc.ca/au-ans/bio_f.asp

[2037] Sur la Commissaire adjointe à la protection de la vie privée du Canada, voy. http://www.priv.gc.ca/au-ans/bio_cb_f.asp

[2038] Sur ce Comité voy. http://www.priv.gc.ca/au-ans/eac_f.asp

569.- Le mode de désignation. Des critiques ont été émises précédemment quant au mode de désignation des membres de la CPVP[2039]. Elles tiennent principalement à la présentation des candidats par le Conseil des ministres.

Pour remédier à ces écueils, il pourrait être judicieux que les membres de la CPVP, ou au moins une partie de ceux-ci, puissent être élus sans être présentés par le Conseil des ministres[2040]. Les candidats à un poste de membre de la CPVP pourraient se présenter devant le Parlement afin d'y exposer les raisons de leur motivation. S'en suivrait un débat public avant la désignation du meilleur candidat élu par les parlementaires.

Par ailleurs, la légitimité des membres de la CPVP élus pourrait être renforcée en prévoyant un vote à majorité spéciale, et non simple, à la Chambre. Ce faisant, les candidats devraient convaincre un plus grand nombre de parlementaires, ce qui renforcerait la voix de l'opposition dans le débat et, dans le même temps, transcenderait la division de la Chambre en groupes linguistiques. Cette idée s'inscrit dans la lignée de la section de législation du Conseil d'État qui a affirmé qu' « il serait souhaitable, en raison des missions confiées à la CPVP, que l'opposition parlementaire soit associée au processus de désignation des membres de la Commission »[2041].

> Cette solution est, par exemple, appliquée en Grèce, où les membres de l'autorité chargée de la protection des données sont désignés par le Parlement après une procédure qui requiert un consentement entre la majorité et l'opposition[2042].
>
> Au-delà des frontières européennes, cette solution est également appliquée au Québec, où les membres de la Commission d'accès à l'information sont nommés par l'Assemblée nationale qui doit approuver leur nomination par un vote d'au moins deux tiers de ses membres[2043].

[2039] Voy. *supra*, n° 503.-

[2040] En ce sens : SLCE du 28 novembre 1990 sur un projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *op. cit.,* n° 1610/1, p. 61 ; SLCE, avis du 2 février 1998 sur un avant-projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *op. cit.,* sess. 1997-1998, n° 1566/1, p. 240.

[2041] SLCE du 28 novembre 1990 sur un projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *op. cit.*, 1610/1, p. 61.

[2042] Art. 16.2 de la loi 2472/1997 on the Protection of the with regard to the Processing of Personal Data disponible sur le site de l'autorité de protection des données héllenique http://www.dpa.gr

[2043] Art. 104 de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

B. L'indépendance institutionnelle de la CPVP

570.- L'octroi de la personnalité juridique à la CPVP. L'indépendance institutionnelle de la CPVP serait renforcée si le législateur[2044] lui octroyait une personnalité juridique propre, comme il l'a déjà fait pour d'autres autorités de régulation.

> Par exemple, l'IBPT[2045], la CREG[2046] et le CSA[2047] ont la personnalité juridique.

En effet, en ayant une personnalité juridique propre, la CPVP jouirait d'une plus grande autonomie de fonctionnement. Cela se marquerait principalement en ce qui concerne la gestion de son budget puisqu'une entité ayant une personnalité juridique distincte de l'État dispose notamment d'un budget indépendant, qui ne doit pas être approuvé par le Parlement[2048]. C'est d'ailleurs l'argument qui a été avancé il y a quelques années pour convaincre le législateur d'octroyer la personnalité juridique au CSA[2049], cette autorité n'en disposant pas jusqu'alors.

> Lors des discussions parlementaires qui ont précédé l'adoption du décret du 27 février 2003 octroyant la personnalité juridique au CSA, il a été avancé que la personnalité juridique « garantira notamment une autonomie de gestion et de fonctionnement au CSA »[2050].

En outre, symboliquement, la personnalité juridique de la CPVP lui permettrait d'affirmer clairement son indépendance.

[2044] Sur la compétence du législateur pour créer une personne morale dictincte de l'État, voy. I. MATHY, « Etre ou ne pas être une personne juridique distincte de l'État, la Communauté ou la Région ? L'autonomie avec ou sans personnalité juridique », *in Le paraétatisme – Nouveaux regards sur la décentralisationfonctionnelle en Belgique et dans les institutions européennes* (dir. P. JADOUL, B. LOMBAERT et F. TULKENS), Bruxelles, la Charte, 2010, p. 41.

[2045] Art. 71 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *M.B.,* 27 mars 1991.

[2046] Art. 23 de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité, *M.B.,* 11 mai 1999.

[2047] Art. 133 de l'arrêté du Gouvernement de la Communauté française du 26 mars 2003 portant coordination du décret sur les services de médias audiovisuels, *M.B.,* 24 juillet 1999.

[2048] I. MATHY, *op. cit.,* pp. 100 et 101 ; M. HERBIET et A.-L. DURVIAUX, *Droit public économique,* Bruxelles, La Charte, 2008, p. 159.

[2049] La personnalité juridique a été attribuée au CSA par l'article 130 du décret du 27 février 2003 sur les services de médias audiovisuels, *M.B.,* 17 avril 2003.

[2050] Projet de décret sur la radiodiffusion, *Doc. Parl.,* Plt C. F., sess. 2002-2003, n° 357-1, p. 3.

Par ailleurs, l'octroi de la personnalité juridique de la CPVP renforcerait la légitimité et l'efficacité de cette institution. Nous y reviendrons[2051].

II. Le renforcement de la légitimité de la CPVP

571.- Une modification du statut de la CPVP. On a vu précédemment que pour renforcer la légitimité de la CPVP, il conviendrait de la responsabiliser davantage en la soumettant à un contrôle politique et à un contrôle juridique, sans pour autant porter atteinte à son indépendance. L'exercice est délicat mais n'est sans doute pas impossible.

A. Organiser le contrôle politique de la CPVP

572.- Deux solutions envisageables. Dans le deuxième chapitre, nous avons souligné la tension qui existe entre la jurisprudence de la Cour de justice de l'Union européenne et celle de la Cour constitutionnelle. La Cour de justice de l'Union européenne s'oppose à l'existence d'un lien si étroit entre le Gouvernement et l'autorité de protection des données qu'il empêcherait cette dernière de faire preuve d'impartialité objective en étant au-dessus de tout soupçon de partialité. En revanche, la Cour constitutionnelle affirme que l'existence d'une autorité indépendante est conforme à la Constitution pour autant que les chambres législatives puissent interpeller un ministre au sujet des agissements de cette autorité[2052].

Pour résoudre cette tension, deux solutions sont envisageables. La première solution tente de concilier ces deux jurisprudences en organisant, tant que faire se peut, un lien entre un ministre et la CPVP. La deuxième solution suppose que la Cour constitutionnelle modifie quelque peu sa jurisprudence.

573.- Première solution : l'organisation d'un lien entre un ministre et la CPVP. Actuellement, la CPVP est rattachée à la Chambre des représentants. Elle n'agit donc pas sous le contrôle d'un ministre. Aucun membre du Gouvernement ne peut donc être interrogé ou interpellé au sujet du fonctionnement de cette autorité de protection des données. Les questions parlementaires relatives à l'action de la CPVP doivent être adressées à cette dernière, ce qui prive la Chambre de la possibilité d'exercer son contrôle politique en ce domaine.

[2051] Voy. *infra,* n° 581.- et n° 595.-
[2052] Voy. *supra,* n° 516.- et s.

> Entre autres exemples, un parlementaire a questionné le Ministre de la Justice après avoir constaté que plusieurs personnes avaient déposé plainte auprès de la CPVP contre « une pratique des syndicats qui enfreignent la loi sur la protection de la vie privée en vue d'écarter des membres ayant des convictions nationalistes flamandes ». Il s'étonnait que cette dernière n'ait toujours pas répondu aux plaintes 18 mois après leur dépôt[2053]. Une autre question parlementaire concerne la lourdeur de la procédure imposée à l'administration flamande pour accéder à des données dépersonnalisées de l'Institut National de Statistique et le fait que « la CPVP, et non l'INS, serait à l'origine de ces difficultés »[2054].
>
> Dans ces cas, le ministre interrogé s'est contenté de suggérer au parlementaire concerné d'interroger directement la CPVP, tout en précisant que le président et les membres de cette autorité « ne reçoivent d'instruction de personne », comme le prévoit l'article 24, §4, de la loi du 8 décembre 1992.

Dès lors, pour organiser le contrôle politique de la CPVP en passant par l'intermédiaire d'un ministre comme le requiert la Cour constitutionnelle, la solution est-elle de revenir à la situation antérieure à la réforme législative du 26 février 2003 en replaçant la CPVP sous le contrôle du Ministre de la Justice ? Certainement pas. Bien que cela soit conforme aux impératifs de notre droit constitutionnel, la directive 95/46 l'en empêche, comme l'a rappelé la Cour de justice de l'Union européenne dans son arrêt du 9 mars 2010 et son arrêt du 16 octobre 2012[2055]. Faut-il alors considérer qu'un contrôle politique de la CPVP est impossible ? Pas nécessairement. Même si la Cour de justice de l'Union européenne insiste sur l'impartialité objective et subjective dont l'autorité de protection des donnés doit faire preuve, elle ne s'oppose pas à ce qu'un lien existe entre ladite autorité et un ministre.

La définition d'une solution suppose tout d'abord qu'on replace la CPVP dans le giron du pouvoir exécutif, de manière à ce qu'un lien puisse être organisé entre la CPVP et un ministre. Séparer la CPVP de la Chambre des représentants n'est pas absurde, et se justifie au regard des éléments qui nous ont poussé à conclure que la CPVP n'est pas un organe collatéral de la Chambre des représentants[2056].

Ensuite, il faut s'interroger sur la consistance du lien entre la CPVP et un ministre. La relation entre la CPVP et un ministre doit incarner un juste milieu entre deux extrêmes. D'un côté, le regard porté par le

---

[2053] Question n° 264 de M. Guy D'haeseleer, du 25 janvier 2010 (N.), *Q.R.*, Chambre, 2009-2010, 22 février 2010, p. 361.

[2054] Question n° 291 de M. Jef Van den Bergh, du 15 janvier 2009 (N), *Q.R.*, Chambre, 2008-2009, 16 mars 2009, pp. 237 et s.

[2055] Voy. *supra*, n° 497.- et n° 511.-

[2056] Voy. *supra*, n° 520.-

ministre sur la CPVP ne doit pas être trop lourd, afin de ne pas s'apparenter à un contrôle de tutelle, interdit par la Cour de justice de l'Union européenne. D'un autre côté, il ne doit pas être trop léger. En effet, si le rôle du ministre se réduit, par exemple, à transmettre le rapport annuel de la CPVP au Parlement, ce dernier n'entretiendrait pas avec la CPVP un lien suffisant pour être capable de répondre aux questions et interpellations de la Chambre au sujet des agissements de la CPVP.

Des réflexions semblables sont menées à l'étranger.

> Comme l'affirme le Conseil d'État français dans un important rapport consacré aux autorités administratives indépendantes, « tous les pays qui ont recouru aux autorités administratives indépendantes ont été confrontés à la nécessité de mettre en place des procédures par lesquelles les organismes administratifs dégagés de la tutelle administrative peuvent rendre compte de leur action aux pouvoirs politiques – législatif, mais aussi exécutif. Cette surveillance n'entrave en rien l'indépendance fonctionnelle qui est reconnue aux autorités administratives indépendantes : elle est au contraire la condition de leur développement et la meilleure garantie de leur bon fonctionnement »[2057]. Et d'ajouter que « si les autorités administratives indépendantes méritent d'exercer leur mission en toute liberté, en particulier lorsque des décisions individuelles sont en cause, l'unité de l'État et la cohérence de l'action publique doivent en effet être préservées. Cela passe notamment par une présence mieux organisée du Gouvernement auprès de certaines autorités administratives indépendantes »[2058].

Actuellement, la loi du 8 décembre 1992 organise déjà un certain lien entre la CPVP et un ministre. Trois dispositions consacrent l'obligation, pour la CPVP, de transmettre la copie de ses avis et de ses recommandations au Ministre de la Justice[2059]. Néanmoins, ces dispositions ont été insérées dans la version initiale de la loi du 8 décembre 1992, lorsque la CPVP était placée sous le contrôle du Ministre de la Justice. Elles n'ont pas été modifiées lors de la réforme législative de 2003. Or, quel est encore le sens de ce lien entre la CPVP et le Ministre de la Justice depuis que la CPVP est rattachée à la Chambre des représentants ? On conçoit difficilement qu'un lien si ténu entre la CPVP et le Ministre de la Justice suffise à justifier l'interpellation de ce dernier du fait des agissements de la CPVP. Rappelons[2060] que c'est d'ailleurs l'interrogation de Michel Pâques au sujet de l'interpellation d'un Ministre du fait des agissements d'une autorité

[2057] Conseil d'État (France), *Rapport public 2001. Les autorités administratives indépendantes*, Études et Documents n° 52, p. 369.

[2058] *Ibid.,* p. 370.

[2059] Voy. les art. 29, §1, 30, §3, et 31, §5, de la loi du 8 décembre 1992.

[2060] Voy. *supra,* n° 516.-

indépendante : si le Ministre « se borne à transmettre un rapport » et n'est que le « débiteur d'un service de transmission de document, comment pourrait-il mal s'en acquitter ? De quelle épaisseur est ce contrôle résiduel ? »[2061].

En revanche, depuis la réforme législative de 2003, l'article 31*bis* de loi du 8 décembre 1992 organise le lien entre « l'institution de gestion du secteur concerné »[2062] et le comité sectoriel compétent pour ce secteur. Le rôle d'institution de gestion est assumé par un service public fédéral[2063]. Chaque comité sectoriel est donc en lien avec un service public fédéral. Ce lien consiste principalement dans le fait que l'institution de gestion du comité sectoriel doit rendre un avis technique et juridique sur les demandes d'autorisation adressées au comité sectoriel[2064]. Néanmoins, la loi n'impose pas au comité sectoriel de suivre cet avis. En outre, le comité sectoriel peut se prononcer même si l'institution de gestion n'a pas rendu d'avis dans le délai imparti. À cet égard également, le lien entre le comité sectoriel et l'administration paraît ténu. Il est difficilement concevable que le Ministre responsable du service public fédéral assumant le rôle d'institution de gestion du comité sectoriel concerné puisse être interpellé du fait des décisions prises par ce comité sectoriel.

Dès lors, pour qu'un ministre puisse être interpellé par les chambres législatives au sujet des agissements de la CPVP, un lien plus consistant doit être créé entre ce ministre et la CPVP. Pour déterminer les différents éléments à partir desquels pourrait s'effectuer le contrôle politique de la CPVP, certaines solutions pratiquées à l'étranger sont intéressantes.

En Belgique, la récente réforme du statut de la CREG mérite également une attention particulière. En effet, s'agissant de la CREG, les directives européennes adoptées en matière d'énergie n'ont longtemps imposé aux régulateurs nationaux qu'une indépendance à l'égard du secteur régulé. Mais, ainsi qu'on l'a déjà dit[2065], en 2009, une nouvelle directive européenne est entrée en vigueur. Elle impose notamment aux États membres de garantir l'indépendance de l'autorité de régulation en veillant « à ce qu'elle exerce ses compétences de manière impartiale et

---

[2061] M. Pâques, « Décentralisation, régulation et contrôle démocratique. L'arrêt 130/2010 en question », *op. cit.,* p. 423.

[2062] Art. 31*bis,* §2, de la loi du 8 décembre 1992.

[2063] Voy. *supra,* n° 492.-

[2064] L'art. 31*bis*, §2, affirme également que « le fonctionnaire dirigeant de l'institution de gestion du secteur concerné peut être invité aux réunions du comité avec voix consultative » et l'art. 31*bis,* §5, dispose que « [...] les comités sectoriels sont établis et se réunissent au siège de la Commission, sauf si l'institution de gestion concernée demande que le comité sectoriel dont elle relève soit établi et se réunisse auprès d'elle ».

[2065] Voy. *supra,* n° 515.-

transparente », que « l'autorité de régulation soit juridiquement distincte et fonctionnellement indépendante de toute autre entité publique ou privée » et qu'elle « puisse prendre des décisions de manière autonome, indépendamment de tout organe politique »[2066]. Cette directive a été transposée en Belgique par une loi du 8 janvier 2012[2067]. Elle intéresse nos réflexions étant donné qu'un parallélisme peut utilement être fait avec l'indépendance qu'impose la directive 95/46 à l'autorité de protection des données, qui, selon la Cour de justice de l'Union européenne, doit également s'interpréter comme l'exercice objectif et impartial du contrôle des traitements de données à caractère personnel.

a) L'audition du ministre. Pour organiser un lien suffisant entre le ministre désigné et la CPVP, il serait judicieux de prévoir que le ministre puisse demander à être entendu par la CPVP sur certaines questions. Lors de cette audition, il pourrait faire part à la CPVP de problématiques nouvelles, ou interroger la CPVP sur les actions qu'elle mène dans tel ou tel domaine pour obtenir des précisions[2068]. Néanmoins, compte tenu de l'arrêt de la Cour de justice de l'Union européenne du 16 octobre 2012, ce droit d'audition ne peut pas être inconditionnel. On devrait, par exemple, prévoir que le ministre doit avancer des raisons justifiant sa demande d'audition. Ce droit ne pourrait pas non plus s'étendre à l'ensemble des agissements de la CPVP. Il importe, en effet, que ce droit ne puisse être utilisé à des fins d'influence politique.

b) Les études et les conseils de la CPVP. Toujours dans l'idée de favoriser le dialogue entre le ministre et la CPVP, le Ministre devrait avoir la possibilité de commander à la CPVP des études sur des points précis. La CPVP devrait aussi pouvoir conseiller le Ministre, d'initiative ou à la demande de ce dernier.

Une règle semblable s'applique à la CREG.

> L'article 23, §2, de la loi du 29 avril 1999 affirme que « La commission est investie d'une mission de conseil auprès des autorités publiques en ce qui concerne l'organisation et le fonctionnement du marché de l'électricité, d'une

[2066] Art. 35 de la directive 2009/72/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur de l'électricité et abrogeant la directive 2003/54/CE et art. 39 de la directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE.

[2067] Loi du 8 janvier 2012 portant modifications de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité et de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations, *M.B.,* 11 janvier 2012.

[2068] En ce sens, voy. Conseil d'État (France), *Rapport public 2001. Les autorités administratives indépendantes, op. cit.*, p. 371.

> part, et d'une mission générale de surveillance et de contrôle de l'application des lois et règlements y relatifs, d'autre part.
>
> À cet effet, la commission :
>
> [...] 2° d'initiative ou à la demande du ministre ou d'un Gouvernement de région, effectue des recherches et des études relatives au marché de l'électricité »
>
> Il en est de même pour la Commission d'accès à l'information du Québec. L'article 174 de la loi sur l'accès à l'information et la protection des renseignements personnels prévoit que le ministre « peut consulter la Commission ». Cette possibilité est justifiée par le fait que « le ministre désigné par le Gouvernement est responsable de l'application de la présente loi. [Il] conseille le Gouvernement en lui fournissant des avis en matière d'accès à l'information et de protection des renseignements personnels, notamment, sur des projets de législation ou de développement de systèmes d'information ».

c) La notification du constat des infractions. Le contrôle politique de la Chambre est souvent initié par la révélation, dans la presse ou par les citoyens, d'infractions commises à l'occasion de certains traitements de données à caractère personnel. Pour pouvoir s'expliquer à ce sujet, le ministre doit avoir connaissance de ces infractions. À cette fin, il faudrait que la CPVP informe le ministre de toute infraction qu'elle constate, ainsi que des solutions qu'elle décide de mettre en place pour y mettre fin voire les sanctionner. Ce faisant, le Ministre pourrait répondre de manière complète aux questions parlementaires.

La CREG est soumise à une même obligation.

> Ainsi, selon l'article 23*bis,* alinéa 2, de la loi du 29 avril 1999 « si la Commission constate, lors de l'exercice de ses tâches de surveillance et de contrôle, des pratiques commerciales déloyales ou un comportement anticoncurrentiel, elle adresse d'initiative au ministre un rapport reprenant ses constatations et, le cas échéant, toute mesure qu'elle estime nécessaire, d'être prise par elle-même ou tout autre autorité compétente, en vue de remédier à des pratiques commerciales déloyales ou à un comportement anticoncurrentiel ayant un effet ou susceptibles d'avoir un effet sur un marché de l'électricité performant en Belgique ».

574.- Deuxième solution : le contrôle de la Chambre des représentants sur le CPVP. Rappelons que la Cour de justice de l'Union européenne s'oppose à ce que le Gouvernement influence le fonctionnement de l'autorité de protection des données. En revanche, elle ne s'oppose pas à une certaine influence parlementaire sur cette autorité et affirme même que « la directive 95/46 n'impose en rien aux États membres une telle absence de toute influence parlementaire »[2069]. Ainsi, le législateur

[2069] § 43 de l'arrêt du 9 mars 2010.

peut définir les compétences de l'autorité de protection des données, les membres de cette autorité peuvent être nommés par le Parlement. On peut également imposer à l'autorité de protection des données une obligation de rendre compte de ses activités au Parlement[2070].

Cette solution consisterait donc à organiser une interaction directe entre le Parlement et la CPVP[2071].

La mise en œuvre de cette solution suppose que la Cour constitutionnelle revienne sur la solution prônée dans son arrêt n° 130/2010 en renonçant à ce que le contrôle politique de la CPVP passe nécessairement par l'intermédiaire d'un ministre. Elle devrait admettre que la légitimité démocratique de la CPVP peut être fondée sur l'existence d'un lien suffisamment étroit entre le Parlement et la CPVP imposant à cette dernière de rendre compte de ses agissements devant les assemblées démocratiques. Remarquons d'ailleurs que l'inexistence d'un lien entre un ministre et la CPVP n'empêche pas que cette autorité puisse être soumise au contrôle du Conseil d'État. Des arrêts récents du Conseil d'État révèlent, en effet, qu'une autorité peut être qualifiée d'autorité administrative même sans être soumise au contrôle du pouvoir exécutif[2072].

En suivant cette solution, le contrôle politique de la CPVP serait plus aisé à mettre en place aujourd'hui. La CPVP ne devrait pas être placée dans le giron du pouvoir exécutif. Elle pourrait demeurer sous l'égide de la Chambre des représentants, puisque la possibilité d'interpeller un ministre ne serait plus exigée. Il conviendrait néanmoins de renforcer le contrôle de la Chambre sur la CPVP afin que la CPVP soit soumise à un contrôle politique d'une certaine consistance. La CPVP serait alors responsable seule devant la Chambre sans passer par l'interpellation d'un ministre.

Pour donner une réelle consistance au contrôle de la Chambre sur la CPVP, il serait intéressant d'imposer à la CPVP de rédiger un *rapport annuel particulièrement précis*. On ne peut qu'insister sur l'importance d'un rapport annuel de qualité. Ce document doit refléter le plus fidèlement possible la réalité de l'activité de l'institution et les problèmes surgissant dans le secteur contrôlé. Comme l'affirme le Conseil d'État français, « le rapport annuel constitue un instrument indispensable à la 'respiration démocratique' d'organismes dotés de compétences décisionnelles. Il est

[2070] Voy. §§ 43 à 46.

[2071] Dans le même sens, Office parlementaire d'évaluation de la législation (France), *Rapport sur les autorités administratives indépendantes,* Sénat, session 2005-2006, n° 404, p. 10.

[2072] Voy. *infra,* n° 575.-

impératif que les autorités administratives indépendantes utilisent toutes les potentialités de cet instrument »[2073].

On regrette que, pour l'heure, les infractions constatées soient présentées d'une manière trop générale pour comprendre concrètement de quoi il s'agissait et comment il y a été mis fin. En effet, la CPVP mentionne le nombre de dossiers traités et traduit ce chiffre en pourcentage. Ces chiffres sont peu éloquents dans la mesure où ils visent tant les dossiers de contrôle, que les dossiers d'information et ceux de médiation[2074]. En outre, la suite qui y a été réservée est formulée de manière trop vague pour être compréhensible, d'autant plus qu'elle n'est reprise que dans un tableau sommaire qui se présente comme suit[2075] :

9.6.1.3 Suite donnée aux dosiers de décision clôturés

Type de dossier	Suite	Nombre	% / type de dossier
Dossiers A	favorable	9	27,27
	favorable avec conditions	15	45,45
	défavorable	4	12,12
	point de vue formulé	1	3,03
	irrecevable	1	3,03
	traitement arrêté	3	9,09
Dossiers AR	point de vue formulé	4	80,00
	traitement arrêté	1	20,00
Dossiers EVAL	point de vue formulé	12	100,00
Dossiers LV	favorable	14	100,00

Par ailleurs, le rapport de la CPVP ne doit pas seulement être un moyen pour cette institution de justifier son existence et la nécessité du budget qui lui est alloué. Cela présenterait peu d'indication sur les agissements concrets de la CPVP et, au-delà, sur les failles existantes dans la protection de la vie privée des citoyens. Ce rapport devrait donc non seulement contenir un exposé du travail effectué par la CPVP, mais également souligner les réels problèmes existant dans l'e-gouvernement notamment, de manière assez détaillée et percutante pour convaincre le législateur et le Gouvernement de réagir aux dangers naissants.

[2073] Conseil d'État (France), *Rapport public 2001. Les autorités administratives indépendantes, op. cit.*, p. 372.

[2074] CPVP, Rapport annuel 2011, p. 78.

[2075] Ce tableau est disponible à la page 83 et ne mentionne malheureusement pas la traduction des termes « dossier A » « dossier AR », « dossier EVAL », « dossier LV ».

À cet égard, la comparaison entre la CPVP et la CREG est éloquente.

> S'agissant de la CPVP, l'article 32, §2, de la loi du 8 décembre 1992 prévoit que « la Commission communique chaque année aux Chambres législatives un rapport sur ses activités. À côté de l'information générale relative à l'application de la présente loi et aux activités de la Commission, ce rapport, qui a un caractère public, contient de l'information spécifique sur l'application des articles 3, §§ 3 et 6, 13, 17 et 18 ».
>
> La même obligation est formulée de manière bien plus précise pour la CREG puisque l'article 23, §3, prévoit que « la commission établit chaque année un rapport annuel qu'elle transmet avant le 1er mai de l'année suivant l'exercice concerné à la Chambre des représentants. Le rapport annuel de la commission porte sur :
>
> 1° l'exécution de ses missions ;
>
> 2° l'état de ses frais de fonctionnement et de leur mode de couverture, y compris une situation actif/passif et le rapport du réviseur d'entreprises ;
>
> 3° l'évolution du marché de l'électricité ;
>
> 4° les mesures prises et les résultats obtenus pour chacune des missions énumérées au § 2 ;
>
> 5° une analyse du plan de développement établi par le gestionnaire du réseau en application de l'article 13, du point de vue de sa cohérence avec le plan de développement du réseau dans l'ensemble de la Communauté européenne visé à l'article 8, § 3, point b), du Règlement (CE) n° 714/2009, ainsi que, le cas échéant, des recommandations de modification du plan de développement établi par le gestionnaire du réseau. La commission tient compte dans le cadre de cette analyse de l'étude prospective établie en application de l'article 3 ;
>
> 6° copie des décisions éventuellement prises pendant l'exercice concerné en matière de méthodologie de calcul des tarifs en application des articles 12 et 12bis.
>
> La commission décrit dans son rapport la manière dont elle a atteint les objectifs formulés dans sa note de politique générale ainsi que dans les orientations générales édictées par le Gouvernement. Elle explique, le cas échéant, les raisons pour lesquelles ces objectifs n'ont pas pu être atteints.
>
> Ce rapport est publié sur le site Internet de la commission. Une copie est également envoyée, pour information, au ministre ».

Il serait également judicieux de prévoir que le rapport annuel de la CPVP doit non seulement être communiqué à la Chambre, mais doit aussi être suivi de la *désignation d'une commission parlementaire* chargée d'étudier ce document et de communiquer à la Chambre les points méritant un écho au sein des assemblées démocratiquement élues.

> C'est, par exemple, une solution mise en place au Québec. L'article 119 de la loi d'accès à l'information et la protection des renseignements personnel

> prévoit que « le rapport d'activités [de la Commission d'accès à l'information] est déposé devant l'Assemblée nationale dans les trente jours de sa réception [...]. La commission de l'Assemblée nationale désigne, dans les meilleurs délais, la commission qui fera l'étude du rapport d'activités. La commission désignée doit faire l'étude de ce rapport dans les 60 jours de son dépôt à l'Assemblée nationale ».

La Chambre devrait aussi pouvoir se prononcer sur la *révocation des membres de la CPVP*, en cas de manquements graves de leur part[2076]. Dès lors, il conviendrait de prévoir l'élection, par la Chambre, d'un Conseil disciplinaire composé de personnes indépendantes. Après avoir mené une procédure respectueuse des droits de la défense, le Conseil disciplinaire rendrait un avis au Ministre responsable de la CPVP, concluant qu'il y a lieu, ou non, de mettre fin prématurément aux fonctions du commissaire. Le Ministre formulerait alors une proposition au Conseil des ministres, sur la base de cet avis.

C'est d'ailleurs la procédure mise en place récemment pour la CREG[2077]. La section de législation du Conseil d'État a insisté sur l'importance qu'un organe parlementaire – et non le Ministre seul – apprécie la nécessité de destituer un membre. Selon elle, la destitution d'un membre ne peut pas avoir lieu sans l'accord de l'instance parlementaire, en l'occurrence, le Conseil disciplinaire. Par contre, même si l'instance parlementaire aboutit à la conclusion qu'un membre doit être destitué, le Ministre n'est pas obligé de suivre cet avis. En d'autres termes « un membre ne peut être révoqué, et son indemnité de sortie annulée, que si la commission a marqué son accord sur une telle décision »[2078].

B. Organiser le contrôle juridictionnel et la transparence de la CPVP

575.- La qualification d'autorité administrative et l'octroi de la personnalité juridique. Le deuxième chapitre[2079] a montré la nécessité d'organiser un recours juridictionnel contre les décisions de la CPVP, et de soumettre les documents qu'elle détient aux obligations de trans-

[2076] Tel serait le cas, par exemple, d'un commissaire faisant preuve d'un manque manifeste d'indépendance.

[2077] Art. 24, §2*bis* et §2*ter,* de la loi du 29 avril 1999.

[2078] SLCE, avis n° 49.570/3 du 31 mai 2011 sur un avant-projet de loi portant modifications de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité et de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations, *Doc. Parl.*, Ch. Repr., session 2010-2011, n° 53-1725/001, p. 312.

[2079] Voy. *supra,* n° 522.-

parence. Qualifier la CPVP d'*autorité administrative* répondrait à ces objectifs. Les décisions de la CPVP pourraient ainsi être soumises à la censure du Conseil d'État, tandis que la loi du 11 avril 1994 sur la publicité de l'administration et la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs s'appliqueraient à notre autorité de protection des données.

Par ailleurs, nous avons précédemment souligné que l'octroi de la *personnalité juridique* à la CPVP renforcerait l'indépendance institutionnelle de cette dernière. Cela aurait également des conséquences sur le contrôle juridictionnel de la CPVP, qu'il convient d'analyser.

Ces deux aspects de la responsabilisation de la CPVP retiennent notre attention dans les lignes qui suivent.

§1. La qualification d'autorité administrative de la CPVP

576.- Des solutions. On a montré précédemment que, telle qu'elle est organisée actuellement, la CPVP ne répond pas à l'ensemble des critères de l'autorité administrative. Bien qu'elle soit instituée par le législateur, qu'elle exerce une mission d'intérêt général, et qu'elle puisse prendre des décisions obligatoires à l'égard des tiers, la CPVP n'est pas soumise à un réel contrôle des pouvoirs publics.

Doit-on pour autant dénier la qualité d'autorité administrative à cette institution ? Nous ne le pensons pas. Deux solutions jurisprudentielles sont envisageables. En outre, si ces solutions devaient ne pas convaincre, l'intervention du législateur pourrait encore être envisagée.

1. Des solutions jurisprudentielles

577.- La pondération des critères. Saisi d'un recours en annulation contre une décision de la CPVP, le Conseil d'État pourrait se déclarer compétent pour connaître de ce recours en qualifiant la CPVP d'autorité administrative alors même qu'elle n'est pas soumise au contrôle des pouvoirs publics.

On peut raisonnablement envisager cette solution en constatant que, dans plusieurs arrêts récents, le Conseil d'État semble porter davantage d'attention au critère de la création par les pouvoirs publics qu'à celui du contrôle par ceux-ci. Ainsi, le Conseil d'État affirme-t-il que « les personnes morales créées par les pouvoirs publics, fût-ce sous une forme de droit privé, aux fins d'assurer une mission de service public [...] sont parties intégrantes de l'administration, et qu'elles peuvent être qualifiées d'autorité administrative, même si elles ne sont pas fondées à prendre des

décisions obligatoires vis-à-vis de tiers »[2080]. En d'autres termes, dans ces arrêts, le Conseil d'État se fonde sur le critère de la création par les pouvoirs publics et celui de l'exercice d'une mission d'intérêt général pour qualifier l'institution d'autorité administrative. En revanche, le critère du contrôle par les pouvoirs publics est passé sous silence. Plus encore, l'absence de pouvoir de décision dans le chef de l'institution n'empêche pas que celle-ci soit qualifiée d'autorité administrative.

Cette jurisprudence devrait être appliquée à la CPVP pour qualifier celle-ci d'autorité administrative, puisque la CPVP est également une personne morale créée par les pouvoirs publics et qu'elle exerce une mission de service public. Par ailleurs, un argument *a fortiori* convainc d'admettre que la CPVP est une autorité administrative : puisque le Conseil d'État considère que des personnes morales créées par les pouvoirs publics et assumant une mission de service public sont des autorités administratives « même si elles ne sont pas fondées à prendre des décisions obligatoires vis-à-vis des tiers », *a fortiori* faut-il reconnaître cette qualité à la CPVP qui dispose d'un tel pouvoir de décision.

L'objectif que poursuivait le législateur lors de la réforme de la CPVP opérée par la loi du 26 février 2003[2081] doit également convaincre le Conseil d'État que la CPVP est une autorité administrative, même si elle n'est pas soumise au contrôle des pouvoirs publics. En effet, avant la réforme de 2003, la CPVP était instituée auprès du Ministère de la justice. La section de législation du Conseil d'État l'avait d'ailleurs qualifiée jadis d' « autorité administrative indépendante »[2082]. En 2003, ce sont principalement des raisons budgétaires qui ont convaincu le législateur de sortir la CPVP du giron du pouvoir exécutif et de l'instituer auprès de la Chambre des représentants. En revanche, ni la composition de cette autorité, ni son mode de fonctionnement ni ses missions n'ont été modifiées. En particulier, les décisions rendues par elle aujourd'hui sont semblables à celles qu'elle rendait avant la modification législative du 26 février 2003. Il s'agit toujours de décisions contraignantes à l'égard des tiers, rendues

[2080] C.E., *SA Energys,* n° 213.949, du 17 juin 2011, p. 8 ; C.E., *Fédération des mutualités socialistes du Luxembourg,* n° 220.232, du 6 juillet 2012, p. 4 ; C.E., *SCRL Établissements Guy Magermans et Cie,* n° 219.043, du 25 avril 2012, p. 5.

[2081] Voy. *supra,* n° 487.-

[2082] Voy. les avis 24.884/2 du 19 février 1996, sur un projet devenu l'arrêté royal n° 12*bis* du 12 mars 1996 modifiant l'arrêté royal n° 12 du 7 mars 1995 relatif à la contribution à verser lors de la déclaration des traitements de données à caractère personnel à la CPVP, cité par l'Auditeur R. Wimmer dans son rapport sur le recours en annulation introduit dans l'affaire *A.-M. Lizin c. CPVP*, du 17 décembre 2010.

par la CPVP dans le cadre de l'exécution de sa mission d'intérêt général[2083]. On doit en conclure que, par la réforme de 2003, le législateur a voulu renforcer les moyens financier de la CPVP, mais il n'a pas souhaité faire échapper cette autorité au contrôle du Conseil d'État ni aux obligations de transparence imposées aux autorités administratives. Il n'aurait d'ailleurs pas pu vouloir un tel changement car il est tenu d'agir conformément au droit européen.

La Cour constitutionnelle l'a encore rappelé dans son arrêt n° 130/2010 à propos d'une autre autorité administrative indépendante, la CREG[2084].

> La Cour constitutionnelle affirme que c'est « en exécution et dans les limites du droit de l'Union européenne » que « le législateur est compétent pour régler les missions et le fonctionnement de la CREG »[2085].

Or, rappelons-le, en vertu de la directive 95/46, un recours juridictionnel doit pouvoir être formé contre les décisions de la CPVP. Dès lors, si le législateur avait voulu soustraire la CPVP du contrôle du Conseil d'État, il aurait dû organiser une voie de recours spécifique, ce qu'il n'a pas fait. Il faut donc admettre que le Conseil d'État est compétent pour connaître des recours intentés contre les décisions de la CPVP.

L'Auditeur au Conseil d'État, Roger Wimmer, abonde en ce sens. Il affirme qu'« une attitude trop frileuse de la part de la section du contentieux administratif du Conseil d'État aurait pour effet paradoxal d'aboutir, par l'évolution du droit de l'Union européenne visant à assurer l'efficacité et la fiabilité du contrôle du respect des dispositions en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel, à une régression importante de la protection juridique, également garantie par le droit de l'Union européenne, à l'égard des actes émanant de l'autorité de contrôle compétente pour la surveillance du traitement des donnés à caractère personnel »[2086].

578.- La qualification par assimilation. L'incertitude qui entoure le statut de la CPVP pourrait convaincre le Conseil d'État de dénier à la

---

[2083] Avant l'intégration des comités sectoriels au sein de la Commission, cette dernière rendait déjà des décisions. On pense, par exemple, au refus d'accès à des documents détenus par elle. L'intégration, au sein de la Commission, des comités sectoriels dotés d'un pouvoir de décision n'a pas apporté de modification à ce constat. Elle l'a simplement amplifié étant donné que, depuis lors, les décisions rendues par la Commission sont bien plus nombreuses qu'auparavant.

[2084] À propos de cet arrêt, voy. *supra,* n° 515.-

[2085] C.C., arrêt n° 130/2010 précité, B.7.1.

[2086] Voy. le rapport de l'Auditeur R. Wimmer précité, pp. 14 et 15, note 13.

CPVP la qualité d'autorité administrative. Même dans cette hypothèse, on ne doit pas pour autant se résigner à admettre que la CPVP ne peut pas être soumise au régime juridique s'imposant d'ordinaire aux autorités administratives. En effet, il peut être recouru à la technique de la qualification par assimilation. Celle-ci se définit comme une « fiction juridique [qui] consiste [...] à rattacher délibérément à une catégorie juridique un objet qui, aux yeux de l'observateur avisé, ne remplit pas les conditions traditionnellement nécessaires pour y entrer, de façon à permettre la mise en œuvre des conséquences attachées à cette catégorie »[2087]. Cette technique de qualification se fonde sur un raisonnement par analogie.

En l'occurrence, supposons que le Conseil d'État estime que la CPVP ne répond pas aux conditions nécessaires pour entrer dans la catégorie juridique de l'autorité administrative. On constate cependant que la CPVP « ne présente pas de différence fondamentale »[2088] avec les institutions traditionnellement qualifiées d' « autorité administrative ». On a vu, en effet, que la CPVP répond à trois des quatre critères de l'autorité administrative. C'est pourquoi, on applique à la CPVP le régime juridique applicable aux autorités administratives. Cette assimilation ne se fonde pas sur une identité réelle entre la CPVP et les institutions traditionnellement qualifiées d'autorités administratives. Elle se justifie par une identité de raison juridique : le but que l'on poursuit en soumettant les décisions des autorités administratives au contrôle du Conseil d'État est similaire à celui qui justifie le contrôle des décisions de la CPVP.

Plus particulièrement, s'agissant de la question de savoir si le Conseil d'État est compétent pour se prononcer sur la légalité d'une décision de la CPVP, on pourrait raisonner comme suit. Le Conseil d'État a été institué « en tant que juridiction spécifique en vue d'offrir une protection juridictionnelle supplémentaire à celle des cours et tribunaux contre les actes administratifs entachés d'illégalité »[2089]. Cette juridiction œuvre à la protection des citoyens à l'égard des décisions arbitraires qui s'appliqueraient à eux[2090]. Elle contribue ainsi à « assurer la sujétion des pouvoirs publics

---

[2087] C. Vautrot-Schwarz, *La qualification juridique en droit administratif,* Paris, L.G.D.J., 2009, pp. 432 et 433. Voy. égal. D. De Roy, « Établissements publics, organismes d'intérêt public et *tutti quanti* : la qualification juridique des satellites de l'administration », note sous Cass. 19 mars 2010, *R.C.J.B.,* 2013, pp. 88 et s.

[2088] *Ibid.,* p. 435.

[2089] C.C., arrêt n° 31/96 du 15 mai 1996, B.2.1.

[2090] E. Maron, « Les notions d'acte administratif et d'autorité administrative : compétence ou incompétence du Conseil d'État pour connnaître des recours en annulation dirigés contre les actes de nature administrative accomplis par des autorités relevant du pouvoir législatif ou du pouvoir judiciaire ? », *in Le Conseil d'État de Belgique. Cinquante ans après sa création (1946 à 1996),* Bruxelles, Bruylant, 1999, p. 328.

à la légalité et à faire ainsi de l'État de droit une réalité plus tangible dans notre pays »[2091].

Or, les décisions de la CPVP s'apparentent en de nombreux aspects aux décisions émanant d'une autorité administrative. Les personnes soumises à une décision illégale de la CPVP pourraient subir le même dommage que les individus visés par une décision illégale émanant d'une autorité administrative. La CPVP doit donc pouvoir être rattachée à la catégorie juridique de l'autorité administrative, afin que chaque personne visée par une décision de la CPVP puisse soumettre celle-ci à l'examen du Conseil d'État et ne pas avoir à subir les conséquences néfastes d'une décision entachée d'illégalité.

Un raisonnement semblable peut être mené s'agissant de la soumission de la CPVP aux obligations de transparence. En effet, les discussions préparatoires relatives au droit fondamental à la transparence administrative, devenu l'actuel article 32 de la Constitution, convainquent de ne pas réserver ce régime juridique à un nombre trop étroit d'institutions. Il a été affirmé qu' « étant donné qu'en l'occurrence il s'agit de l'octroi d'un droit fondamental, une interprétation aussi large que possible [de la notion d'autorité administrative] devra être utilisée. On peut notamment[2092] renvoyer à l'article 14 des lois sur le Conseil d'État et la jurisprudence du Conseil d'État à ce sujet »[2093]. En particulier, la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs a été adoptée pour offrir « une meilleure protection au citoyen »[2094], notamment parce que « le requérant informé des motifs d'un acte contesté sera plus à même d'organiser ses moyens » et que la motivation formelle « constitue le gage d'un examen sérieux et impartial de l'affaire »[2095]. Par ailleurs, les discussions préparatoires à l'adoption de la loi du 11 avril 1994 sur la publicité de l'administration insistent sur l'importance de la transparence administrative pour mettre en œuvre une « réorientation fondamentale

[2091] B. Blero, « Introduction générale », in *Le Conseil d'État de Belgique. Cinquante ans après sa création (1946-1996), op. cit.*, p. 5.

[2092] C'est nous qui soulignons.

[2093] Proposition du Gouvernement visant à insérer un article 24*ter* dans la Constitution relatif à la publicité de l'administration, Note explicative, *Doc. Parl.,* Ch. repr., session 1992-1993, n° 839/1, p. 5.

[2094] Projet de loi relatif à la motivation formelle des actes administratifs, Rapport fait au nom de la Commissionde l'Intérieur, des affaires généralesn de l'éducation et de la fonction publique par M. Timmermans, *Doc. Parl.,* Ch. Repr., session 1990-1991, n° 1595/4, p. 2.

[2095] Proposition de loi relative à la motivation formelle des actes administratifs, Développements, *Doc. Parl.,* Sénat, sess. extr. 1988, n° 215-1, p. 1.

de la relation entre le citoyen et l'administration », en renforçant notamment « le citoyen dans la défense de ses droits »[2096].

Compte tenu de l'importance d'envisager largement les autorités soumises aux obligations de transparence, la CADA et le Conseil d'État devraient reconnaître que la CPVP est tenue de respecter l'article 32 de la Constitution, la loi du 11 avril 1994 sur la publicité de l'administration ainsi que la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs.

> Un exemple de qualification par assimilation peut être trouvé dans un arrêt relativement récent de la Cour de cassation[2097]. À l'origine de cette affaire, un agent de l'administration de la T.V.A. communique à l'Institut des experts-comptables une information relative au comportement possiblement frauduleux d'un expert-comptable. La question se pose de savoir si, en communiquant ladite information, l'agent de l'administration de la T.V.A. a respecté l'article 93, *bis,* du Code de la TVA. Cette disposition impose une obligation de secret professionnel aux agents de l'administration de la T.V.A. tout en affirmant que cette obligation ne s'applique pas lorsque, notamment, les renseignements sont communiqués à un « organisme public ». Cela signifie qu'en l'espèce l'agent n'a pas violé l'article 93 *bis* du Code de la TVA en communiquant ladite information à l'Institut d'experts-comptables, pour autant que l'Institut d'experts-comptables puisse être qualifié d'organisme public au sens du Code de la TVA. Pour clarifier la qualification à donner à l'Institut d'experts-comptables, la Cour de cassation reconnaît qu'en raison de l'indépendance dont il bénéficie, l'Institut des experts-comptables ne répond pas à la définition d'organisme public donnée par le Code de la TVA. La Cour se réfère néanmoins à la raison juridique de ces dispositions. Ainsi, il transparaît des travaux préparatoires que « le législateur a, pour combattre non seulement la fraude fiscale mais aussi les infractions à des législations ou réglementations non fiscales, entendu la notion d'organisme public dans une acception large ». Elle affirme qu'un groupement professionnel de droit public, tel que l'Institut des experts-comptables doit « en dépit de l'indépendance dont il bénéficie, être considéré comme un organisme public pour l'application de l'article 93*bis* du Code de la TVA »[2098].

[2096] Exposé des motifs du projet de loi relatif à la publicité de l'administration, *Doc. Parl.,* Ch. Repr., session 1992-1993, n° 1112/1, pp. 1 et 2.

[2097] Cass., 19 mars 2010, C.05.0197.F/1. Pour une analyse de cet arrêt et de cette problématique en général, voy. D. De Roy, « Établissements publics, organismes d'intérêt public et *tutti quanti* : la qualification juridique des satellites de l'administration », *op. cit.*, pp. 34 à 97.

[2098] *Ibid.*, feuillet n° 16.

2. Une solution législative

579.- La qualification légale d'autorité administrative. Le législateur pourrait reconnaître à la CPVP la qualification d'« autorité administrative au sens de l'article 14 des Lois sur le Conseil d'État, coordonnées le 12 janvier 1973 » et insérer cette qualification dans la loi du 8 décembre 1992. L'éventuelle reconnaissance, par le Conseil d'État, de la qualité d'autorité administrative de la CPVP pourrait d'ailleurs l'encourager à franchir cette étape.

Il s'agirait d'une qualification par référence[2099], puisque la loi du 8 décembre 1992 qualifierait la CPVP en se référant à une autre norme, en l'occurrence, l'article 14 des Lois coordonnées sur le Conseil d'État. Le procédé de la qualification par référence est déjà utilisé par le législateur, notamment dans la loi du 29 juillet 1991 sur la motivation formelle des actes administratifs[2100].

Grâce à une telle qualification, les décisions de la CPVP pourraient, sans hésitation, faire l'objet d'un recours au Conseil d'État. La CPVP serait également soumises aux obligations de transparence applicables aux autorités administratives au sens de l'article 14 des lois coordonnées sur le Conseil d'État.

580.- La modification de l'article 14 des lois coordonnées sur le Conseil d'État. Si ni le Conseil d'État, ni le législateur, ne reconnaissent à la CPVP la qualité d'autorité administrative, une autre solution consiste, pour le législateur, à compléter l'article 14 des Lois coordonnées sur le Conseil d'État qui définit les actes soumis au contrôle du Conseil d'État, section du contentieux administratif. Cette disposition pourrait prévoir que les actes de la CPVP peuvent aussi être soumis à ce contrôle, au même titre que les décisions des autorités administratives.

Un ajout semblable a déjà eu lieu. Des fonctionnaires des assemblées législatives ont jadis posé la question à la Cour constitutionnelle de savoir s'il n'était pas discriminatoire de les priver de recours contre les décisions les concernant au motif qu'ils ne faisaient pas partie d'une autorité administrative. La Cour a reconnu l'existence d'une discrimination tout en relevant que celle-ci ne pourrait être résorbée « que par une intervention du législateur, lors de laquelle il puisse envisager, par égard à l'indépendance

[2099] À ce sujet, voy. D. De Roy, « Établissements publics, organismes d'intérêt public et *tutti quanti* : la qualification juridique des satellites de l'administration », *op. cit.,* pp. 47 et s.

[2100] Voy. l'article 2, lu en combinaison avec l'article 1er : l'obligation de motivation formelle est imposée aux « autorités administratives » visées à l'article 14 des Lois sur le Conseil d'État, coordonnées le 12 janvier 1973.

qui doit être assurée aux assemblées législatives, de prévoir des garanties spécifiques auxquelles il n'a pas dû veiller lors de l'élaboration des lois coordonnées sur le Conseil d'État. [...] Il résulte de ce qui précède que [...] la discrimination ne trouve pas son origine dans l'article 14, mais dans une lacune de la législation, à savoir le défaut d'organisation d'un recours en annulation des actes administratifs des assemblées législatives ou de leurs organes »[2101]. Depuis la loi du 25 mai 1999, le Conseil d'État peut connaître des actes administratifs des assemblées législatives ou de leurs organes, en ce compris les médiateurs institués auprès de ces assemblées, de la Cour des comptes et de la Cour d'arbitrage, ainsi que des organes du pouvoir judiciaire et du Conseil supérieur de la justice relatifs aux marchés publics et aux membres de leur personnel.

En l'espèce, une même lacune de la législation, concernant cette fois les actes administratifs de la CPVP, pourrait amener le législateur à réagir une nouvelle fois. C'est d'ailleurs le souhait que la CADA a formulé récemment à propos des comités sectoriels[2102].

§2. La responsabilité individuelle de la CPVP

581.- L'octroi de la personnalité juridique à la CPVP. Le contrôle juridictionnel de la CPVP gagnerait à ce que cette institution dispose d'une personnalité juridique propre, pour deux raisons principalement.

La première raison est d'ordre *procédural*. Actuellement, pour mettre en cause la responsabilité de la CPVP, il y a lieu d'assigner l'État, étant donné que la CPVP n'est pas un organisme personnalisé. Comme l'affirme Irène Mathy, « il en résulte, certainement, une rigidité plus importante dans la capacité de réaction du service non personnalisé aux 'attaques' qui pourraient être lancées contre son action »[2103]. Si la CPVP était un organisme personnalisé, celle-ci serait citée elle-même comme partie adverse, indépendamment de l'État belge. Elle pourrait elle-même défendre ses décisions.

La deuxième raison concerne l'examen, *au fond*, des actions intentées contre la CPVP. La CPVP serait seule responsable des conséquences de ses actes. Elle serait ainsi tenue de réparer les dommages causés par une décision entachée d'irrégularité ou par une absence d'agir qui serait considérée

[2101] C.C., arrêt n° 31/96 du 15 mai 1996. Sur cet arrêt, voy. E. MARON, *op. cit.*, pp. 323-328.

[2102] CADA, avis n° 2011-309 du 10 octobre 2011 sur le refus de donner accès à des documents qui ont été utilisés par le Comité sectoriel de la sécurité sociale et de la santé pour prendre une décision, p. 9.

[2103] I. MATHY, *op. cit.*, p. 106.

comme fautive. Une telle responsabilisation de la CPVP ne peut qu'encourager cette dernière à user effectivement des moyens d'action dont elle dispose[2104] et à veiller scrupuleusement à la constitutionnalité et à la légalité des décisions rendues par les comités sectoriels institués en son sein[2105].

Certes, la responsabilisation de la CPVP pourrait contraindre cette dernière à financer un assureur pour être en mesure d'assumer les conséquences économiques d'une possible condamnation, alourdissant d'autant les coûts de fonctionnement de cette institution. C'est d'ailleurs un argument qui a été invoqué, en France, pour décourager l'octroi de la personnalité juridique à la CNIL[2106].

Néanmoins, à notre sens, ce problème financier pourrait être résolu en organisant légalement l'intervention financière de l'État fédéral au cas où les ressources de la CPVP ne suffiraient pas à couvrir le montant des dommages et intérêts qu'elle serait condamnée à payer. Cette solution est déjà organisée pour le CSA.

> S'agissant du CSA, l'article 151(3) de l'arrêté du Gouvernement de la Communauté française du 26 mars 2003[2107] dispose que « chaque année, la Communauté française alloue au CSA, le cas échéant, une dotation complémentaire spécifique. Celle-ci couvre les dommages et intérêts payés par le CSA en raison de la mise en cause éventuelle de sa responsabilité pour des faits relevant de l'exécution de ses missions visées aux articles 159 à 163. La dotation spécifique ne sera versée que dans la mesure où le montant de ces dommages et intérêts ne peut être couvert par les autres ressources du CSA ».

Section 2. Le renforcement de l'efficacité de la CPVP

582.- Un rôle essentiel à perfectionner. La CPVP exerce un rôle essentiel. Comme on l'a dit[2108], elle est une autorité de régulation dont le travail complète utilement les normes générales et abstraites définies par le légis-

---

2104 À ce sujet, voy. *supra,* n° 550.- et *infra,* n° 582.- et s.

2105 À ce sujet, voy. *supra,* n° 534.- et s. et *infra,* n° 596.- et s.

2106 Voy. Office parlementaire d'évaluation de la législation (France), *Rapport sur les autorités administratives indépendantes*, Sénat, session 2005-2006, n° 404, pp. 57 à 61, spéc. p. 61.

2107 Arrêté du Gouvernement de la Communauté franc¸aise du 26 mars 2003 portant coordination du décret sur les services de médias audiovisuels. Cet arrêté du Gouvernement a été ratifié par un décret du 30 avril 2009 (*M.B.,* 24 juillet 2009).

2108 Voy. *supra,* n° 490.-

lateur et par le gouvernement, puisque ces normes ne pourraient suffire à elles seules pour encadrer l'e-gouvernement. L'action de la CPVP se fonde sur des moyens juridiques classiques que sont le pouvoir d'enquête, le pouvoir de dénonciation au procureur du Roi et le pouvoir d'intenter une action d'intérêt collectif. Elle dispose également de moyens d'action plus souples, que sont les avis, les recommandations, la procédure de médiation dans le but de parvenir à une conciliation ainsi qu'un pouvoir d'autorisation exercé par les comités sectoriels.

Dans le deuxième chapitre, on s'est interrogé sur l'efficacité et l'effectivité de ces moyens d'action. Les moyens juridiques classiques ne sont pas ou peu utilisés par la CPVP. Ainsi, le pouvoir d'agir dans l'intérêt collectif manque d'effectivité : il n'a jamais été utilisé par la CPVP alors qu'il pourrait l'être pour sanctionner les administrations qui traitent illégalement des données. Quant au pouvoir de dénonciation au Procureur du Roi, il n'est pas adapté à l'e-gouvernement puisqu'il ne pourrait pas être utilisé à l'égard d'une administration, l'État étant pénalement irresponsable.

Quant aux autres moyens d'action, ils sont effectivement utilisés. La CPVP rend de nombreux avis et recommandations ; les comités sectoriels prennent régulièrement des décisions pour autoriser ou refuser des échanges de données dans l'administration. Néanmoins ces moyens sont-ils suffisamment efficaces pour contrôler l'e-gouvernement ? On peut en douter en constatant que rien n'oblige le législateur, le Gouvernement ou les administrations à se conformer aux avis et aux recommandations de la CPVP. Quant aux décisions des comités sectoriels, elles sont contraignantes mais la CPVP ne dispose pas d'un pouvoir d'amende pour sanctionner l'administration qui ne s'y conformerait pas. Concrètement, cela signifie que les traitements de données illégaux effectués dans l'administration sont donc peu, voire pas, sanctionnés.

Une autre voie de contrôle est la saisine des cours et tribunaux par les citoyens victimes d'un traitement de données illégal. Ce moyen d'action manque lui aussi d'effectivité. On constate, en effet, que les citoyens n'usent pas des voies de recours traditionnelles pour attaquer ces illégalités à la Cour constitutionnelle, au Conseil d'État ou devant le juge judiciaire. Probablement est-ce dû au fait que les personnes concernées n'ont ni le courage ni les moyens d'agir en justice pour sanctionner ce type de problème[2109]. De manière plus générale, on observe aussi que les arguments juridiques tirés du régime de la protection des données sont peu invoqués dans les litiges qui mettent en cause la légalité d'une décision

[2109] À ce sujet, voy. les développements relatifs à l'utilité, dans l'e-gouvernement, de l'action d'intérêt collectif qui peut être menée par la CPVP, *supra,* n° 550.-

administrative, comme si les requérants « oubliaient » l'existence et la richesse de ces règles[2110]. En outre, quand ces règles sont invoquées, elles ne sont pas toujours bien exploitées[2111].

Moyennant certaines améliorations, l'action de la CPVP pourrait contribuer à améliorer cette situation. D'une part, la CPVP pourrait faire connaître davantage l'importance et la richesse des règles de protection des données. Certaines actions sont déjà menées mais gagneraient à être amplifiées pour toucher davantage le public. D'autre part, les moyens de contrôle à disposition de la CPVP doivent être renforcés.

I. Un renforcement de la mission d'information

583.- La mission d'information de la CPVP. Ainsi qu'on l'a déjà évoqué, la CPVP rédige un rapport annuel d'activité, gère un site web, répond aux questions qui lui sont adressées, mène des campagnes de sensibilisation sur les questions de protection de la vie privée, etc.[2112]. Ce sont autant d'actions qui entrent dans sa mission d'information du public. Néanmoins, elles pourraient être améliorées à certains égards. Il serait ainsi bénéfique que la CPVP clarifie certains documents dont elle est l'auteure, multiplie les interventions publiques, et guide les modifications législatives.

584.- Clarifier les documents. Nombreuses sont les situations dans lesquelles les avis, les recommandations et les autorisations de la CPVP sont particulièrement utiles pour éclairer les personnes intéressées sur la légalité des traitements de données mis en place dans notre pays.

> Par exemple, un citoyen s'étonne que la Région wallonne ait eu accès à la copie de son permis de bâtir détenu par sa commune, un avocat est mandaté pour attaquer une nouvelle loi organisant un traitement de données à

[2110] À ce sujet, voy. Bruxelles (9e ch.), 9 mai 2012, *J.T.*, 2012, p. 691, obs. E. Degrave, « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données à caractère personnel illégal sanctionné par la Cour d'appel de Bruxelles ». Dans cette affaire, les demandeurs ont manqué d'invoquer les règles de protection des données à caractère personnel devant le tribunal de première instance. Ils ont été déboutés de leur demande. Par contre, ils ont invoqué ces règles en appel, ce qui a abouti à la condamnation de l'intimé, responsable de traitement.

[2111] Pour un exemple, voy. *supra,* n° 445.-

[2112] Voy. les informations données à ce sujet par la CPVP sur son site internet www.privacycommission.be, onglet « vision et mission ».

caractère personnel[2113], un parlementaire est inquiet de l'utilisation de *Facebook* par les contrôleurs fiscaux, etc.

Pour l'heure, un courage certain est nécessaire pour accéder aux documents pertinents dans cette matière et en comprendre la portée. En effet, l'ampleur de la compétence de la CPVP engendre une jurisprudence très abondante qui peut également être fluctuante à certains égards. Il est vrai que la CPVP est confrontée à l'évolution grandissante des technologies, qui fait naître des risques nouveaux pour la protection de la vie privée et rend nécessaire une certaine adaptation des analyses menées. Le contexte politique peut également expliquer certaines modifications. Il n'empêche que l'abondance des documents émis et les modifications affectant certaines interprétations nuisent à la transparence, à la lisibilité et à la prévisibilité des positions de la CPVP. Des améliorations sont nécessaires.

Un tel impératif pédagogique est d'ailleurs interprété rigoureusement par le Conseil d'État français, dans son rapport public sur les autorités administratives indépendantes.

> Le Conseil d'État français affirme qu' « en marge du rapport annuel, il convient que les autorités administratives indépendantes dotées d'un pouvoir de décision gardent le souci d'éditer des documents clairs et pédagogiques, indiquant les conditions dans lesquelles elles interviennent et précisant le contenu des règles en vigueur, l'interprétation jurisprudentielle qui en a été donnée et la doctrine dont elles entendent faire application, sous le contrôle du juge. Cette édition doit se faire sous forme de documents écrits classiques, mais plus efficacement encore dans le cadre de leur site Internet, appelé à devenir de plus en plus l'instrument privilégié pour porter à la connaissance du public leurs décisions et leur 'politique' »[2114].

Ainsi, il serait appréciable que la CPVP structure ses documents de manière plus homogène, en indiquant les critères sur lesquels elle fonde chaque étape de son analyse. C'est d'ailleurs ce que semblent déjà faire certains comités sectoriels institués au sein de la CPVP.

> Par exemple, le Comité sectoriel pour l'Autorité fédérale adopte une structure semblable pour chaque autorisation émise. Sous un titre « conditions de licéité du traitement », figurent notamment les sous-titres « principe de

[2113] Un exemple a récemment été divulgué par la presse au sujet de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions, *M.B.*, 24 août 2012. Voy. http://www.lalibre.be/economie/actualite/article/757579/la-nouvelle-loi-sur-les-competences-du-fisc-bientot-attaquee.html

[2114] Conseil d'État (France), *Rapport public 2001. Les autorités administratives indépendantes, op. cit.*, p. 372.

finalité », « principe de transparence », « principe de proportionnalité », suivis de l'analyse de la demande au regard de chacune de ces exigences.

S'agissant plus particulièrement des avis, leur compréhension serait également facilitée si la version de la norme en projet, telle que soumise à la CPVP, était jointe à l'avis, à l'image des avis de la section de législation du Conseil d'État relatifs à des normes de valeur législative. Ceux-ci sont précédés de la copie de la norme en projet, telle que soumise à l'autorité consultative. Cela permet d'avoir accès au texte exact examiné, ainsi qu'à la numérotation de celui-ci.

Enfin, il pourrait être utile que soit créé un index reprenant la liste des mots-clés en matière de protection des données à caractère personnel, à côté desquels figurerait le numéro des avis recourant à ceux-ci, voire un résumé de ceux-ci.

Le site internet de la Cour constitutionnelle[2115] offre un exemple intéressant d'outil de ce type. Sous la rubrique « Affaires pendantes et jurisprudence », dans l'onglet « rechercher », figure un document PDF dénommé « Table systématique cumulative de la jurisprudence », qui permet d'accéder aux mots-clés et au numéro des arrêts y relatifs. Sous l'onglet « rechercher », figurent également d'autres outils intéressant, tel qu'un moteur de recherche permettant d'intégrer un mot-clé et d'accéder aux arrêts concernés ainsi qu'à un résumé de ceux-ci.

585.- Multiplier les interventions publiques. Pour faire connaître au mieux son action, la CPVP devrait se montrer plus présente dans les médias. De cette manière, elle pourrait attirer l'attention des citoyens sur l'importance de la protection des données et les droits qui sont les leurs en ce domaine. L'intervention de la CPVP serait également très utile pour signaler les pratiques illégales naissantes afin d'inciter les citoyens à exercer leurs droits, et attirer l'attention des responsables politiques.

Il est surprenant de constater qu'au Québec, la loi sur l'accès à l'information et la protection des renseignements personnels est mentionnée au moins une fois par jour dans la presse[2116]. On est encore loin d'un tel attrait pour la protection des données en Belgique.

[2115] www.const-court.be

[2116] Entretien avec le Commissariat d'accès à l'information du Québec, Montréal, le 16 avril 2012.

586.- Guider les modifications législatives. On a souligné plus haut[2117] la qualité des recommandations de la CPVP. Elles offrent des éclaircissements et des mises au point qui se fondent bien souvent sur des réflexions approfondies acquises au gré de plusieurs expériences en matière d'e-gouvernement. Les synthèses ainsi offertes doivent aider au développement harmonieux de l'e-gouvernement.

Vu l'utilité, voire la nécessité, d'explications sur les concepts nouveaux de l'e-gouvernement, et vu la rareté des normes, de la doctrine et de la jurisprudence qui y sont consacrées, il serait intéressant d'encourager davantage l'adoption de recommandations pour définir et organiser la matière. En particulier, la CPVP pourrait recourir à des recommandations pour évaluer, à intervalles réguliers, l'application de la loi du 8 décembre 1992 en Belgique et dans le secteur public en particulier. Un bilan pourrait être dressé et des solutions concrètes proposées pour améliorer la protection de la vie privée des citoyens dans l'administration.

L'émission, par la CPVP, de recommandations globales à intervalles réguliers pourrait être organisée en s'inspirant de la solution québécoise. En effet, la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels prévoit, en son article 170, que « la Commission doit, [...] tous les cinq ans, faire au Gouvernement un rapport sur l'application de la présente loi [...] ainsi que sur les sujets que le ministre peut lui soumettre ». Ce rapport peut comprendre des recommandations. Suite au dépôt de ce rapport quinquennal, l'Assemblée nationale doit désigner une commission parlementaire, chargée d'étudier ledit rapport, d'auditionner tout représentant des citoyens et des organismes intéressés et d'évaluer l'opportunité de modifier la loi[2118]. Le plus souvent, une révision de la loi s'en suit[2119]. Ce rapport, dont la portée dépasse largement un rapport d'activité, permet de maintenir l'adéquation entre la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et les enjeux sociétaux concrets.

II. Un renforcement des moyens de contrôle de la CPVP

587.- Considérations générales. Les voies de contrôle traditionnel ne permettent qu'un examen *a priori* ou *a posteriori* des traitements de données à caractère personnel. La CPVP pourrait utilement contrôler les traitements

[2117] Voy. *supra*, n° 533.- et s.

[2118] Art. 179.1 de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

[2119] Entretien avec la Directrice des affaires juridiques de la Commission d'accès à l'information du Québec, à Montréal, le 16 avril 2012.

de données en cours d'exécution, si on renforce ses moyens de contrôle en lui octroyant un pouvoir d'injonction, un pouvoir d'admonestation et un pouvoir d'amende, si elle peut agir à la Cour constitutionnelle et au Conseil d'État et si elle dénonce davantage les traitements de données illégaux. Par ailleurs, la procédure d'autorisation par les comités sectoriels semble inutilement lourde. Une autre solution peut être proposée.

A. La dénonciation des traitements illégaux dans le rapport annuel

588.- Un moyen d'assurer le contrôle politique des administrations. La CPVP remet chaque année un rapport d'activité à la Chambre des représentants[2120]. Cet outil permet à la Chambre de contrôler le fonctionnement de la CPVP[2121]. Mais il pourrait également servir aux députés pour contrôler les traitements de données effectués dans les administrations. À cet égard, on regrette que ce rapport ne dénonce pas les illégalités de manière exhaustive, et ne mentionne pas précisément la liste des administrations qui en sont responsables. Cela permettrait aux députés de prendre pleinement connaissance des problèmes et de leur origine, et d'interpeller ensuite les ministres concernés. Le contrôle politique de l'e-gouvernement n'en serait que fortifié.

> Actuellement, le rapport annuel de la CPVP ne fait que mentionner des « domaines », définis de manière assez vagues (autorités publiques, télécommunications, Justice, …)[2122] à propos desquels elle a eu à traiter un dossier.
>
> Toute autre est la confection du rapport annuel du Commissariat à la protection de la vie privée du Canada. Par exemple, le rapport annuel 2007-2008[2123] illustre l'intérêt de disposer d'une liste d'administrations à l'égard desquelles des plaintes ont été déposées pour violation de la loi canadienne relative à la protection des renseignements personnels. Cette liste reprend, pour chaque institution gouvernementale, le total des plaintes déposées à leur égard pour l'année.

[2120] Art. 32, §2, de la loi du 8 décembre 1992.

[2121] Voy. *supra* n° 465.- et not. la question n° 0643 de M. Eric van Weddingen, du 4 avril 2001 (F), *op. cit.*, p. 10470.

[2122] Voy. CPVP, Rapport annuel 2011, pp. 78, 79 et 89.

[2123] Ce rapport est disponible à l'adresse http://www.priv.gc.ca/information/ar/200708/200708_pa_f.pdf

Plaintes reçues par institution gouvernementale

	Total
Service correctionnel du Canada	248
Gendarmerie royale du Canada	84
Agences des services frontaliers du Canada	54
Service Canada	52
Défense nationale	48
Service canadien du renseignement de sécurité	45
Agence du revenu du Canada	38
Société canadienne du Canada	28
Affaires étrangères et Commerce international Canada	27
Justice Canada	18
Ressources humaines et Développement social Canada	14
Citoyenneté et Immigration Canada	14
Santé Canada	8
Transport Canada	7
Travaux publics et Services gouvernementaux Canada	6
Pêches et Océans Canada	5
Bibliothèque et Archives Canada	5
Bureau du Conseil privé	5
Agriculture et Agroalimentaire Canada	4
Agence canadienne d'inspection des aliments	4
Affaires indiennes et du Nord Canada	4
Secrétariat du Conseil du Trésor du Canada	4
Commission des plaintes du public contre la GRC	3
Environnement Canada	3

Extrait du Rapport annuel 2007-2008 du Commissariat à la protection de la vie privée du Canada, p. 106.

> Selon le Commissariat à la protection de la vie privée du Canada, le fait de stigmatiser les administrations fautives dans un rapport public est un moyen efficace pour les inciter à se conformer aux exigences de la protection des renseignements personnels[2124].

Par ailleurs, de telles dénonciations devraient également éclairer les ministres qui exercent un contrôle sur les administrations. En ayant une meilleure connaissance des illégalités commises dans l'administration

[2124] Entretien avec deux commissaires du Commissariat à la protection de la vie privée du Canada, Ottawa, le 10 avril 2012.

dont il est responsable, le ministre concerné pourrait intervenir rapidement auprès de ladite administration pour lui enjoindre de respecter la loi et imposer, le cas échéant, des sanctions disciplinaires aux agents ayant utilisé abusivement les données.

B. L'octroi d'un pouvoir d'injonction, d'un pouvoir d'admonestation et d'un pouvoir d'amende

589.- Considérations générales. Que ce soit pour respecter les obligations de la directive 95/46 ou pour renforcer l'efficacité de l'action de la CPVP, notre autorité de protection des données devrait être dotée d'un pouvoir d'injonction, d'un pouvoir d'amende et d'un pouvoir d'admonestation. Ces trois moyens de contrôle pourraient être appliqués de manière alternative ou cumulative.

§1. Un pouvoir d'injonction

590.- Traitement de données en cours ou terminé. La CPVP devrait disposer d'un pouvoir d'injonction qu'elle pourrait exercer sur un traitement de données en cours et/ou pour sanctionner, *a posteriori,* l'administration responsable d'un traitement de données illégal.

a) Pouvoir d'injonction visant un traitement de données en cours. Le pouvoir d'injonction portant sur un traitement en cours pourrait consister à ordonner le verrouillage, l'effacement ou la destruction des données, ainsi qu'interdire temporairement ou définitivement un traitement. Un tel pouvoir d'injonction permettrait à la CPVP d'obtenir rapidement la cessation de traitements de données illégaux menés dans l'administration et ce, sans attendre qu'un citoyen saisisse les cours et tribunaux. De plus, comme on l'a dit précédemment[2125], l'article 28.3 de la directive 95/46 impose que l'autorité de protection des données nationale dispose d'un tel pouvoir d'injonction. La CPVP est d'ailleurs la seule autorité de protection des données européenne a en être privée[2126]. Il s'impose donc que le législateur mette fin à un tel manquement dans la transposition de la directive européenne.

b) Pouvoir d'injonction visant un traitement de données terminé. En complément d'une injonction visant un traitement de données en

[2125] Voy. *supra,* n° 551.-

[2126] European Union Agency for fundamental rights, Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II, *op. cit.*, p. 23.

cours, ou alternativement à celle-ci, l'injonction exercée par la CPVP pourrait également être utilisée comme un moyen de sanctionner un traitement de données illégal qui a pris fin.

Ainsi, après avoir constaté qu'une administration accomplit des traitements de données illégaux, la CPVP pourrait imposer aux membres de cette administration de suivre une formation relative à la protection des données à caractère personnel. De cette manière, les agents de l'administration acquerraient une connaissance plus approfondie de ce régime juridique. Ils prendraient davantage conscience de l'importance de respecter ces règles et des sanctions encourues en cas de non respect desdites normes.

§2. Un pouvoir d'admonestation

591.- Un avertissement public. Comme le pouvoir d'injonction visant un traitement en cours, le pouvoir d'admonestation devrait déjà avoir été attribué à la CPVP, conformément à l'article 28.3 de la directive 95/46.

Ce pouvoir consiste en la rédaction d'un avertissement à destination d'un responsable de traitement qui ne respecte pas le régime juridique de la protection des données. L'admonestation peut être rendue publique, notamment en la publiant sur le site internet de l'autorité de protection des données.

Ainsi, dans l'hypothèse où une admonestation dénoncerait publiquement les agissements illégaux d'une administration, elle mettrait en cause la réputation de l'administration quant à la manière dont elle traite les données à caractère personnel des citoyens. On peut raisonnablement penser que pareille admonestation constituerait un moyen de pression particulièrement intéressant pour inciter ladite administration à se conformer au régime juridique de la protection des données à caractère personnel. En outre, l'admonestation pourrait être assortie d'une menace d'injonction[2127] ou d'amende[2128] au cas où l'admonestation ne serait pas suivie d'effets.

Ce type de sanction est régulièrement utilisé par la CNIL en France, y compris à l'égard de l'administration[2129]. Lorsque la CNIL prononce un

[2127] Voy. *supra,* n° 590.-

[2128] Voy. *infra,* n° 592.- et s.

[2129] Pour un exemple d'avertissement public adressé par la CNIL à une administration, voy. la délibération n° 2012-320 du 20 septembre 2012 portant avertissement public à l'encontre de la Commune de Montreuil, disponible sur le site www.legifrance.gouv.fr

avertissement public, celui-ci est publié sur son site internet et sur le site internet Legifrance.

§3. Un pouvoir d'amende

592.- Une possible compétence future. La question se pose de savoir si la CPVP devrait être dotée du pouvoir d'imposer une amende administrative aux responsables de traitement qui violeraient la protection des données. Dans l'affirmative, ce pouvoir pourrait être utilisé en sus de l'injonction et de l'admonestation.

La CPVP ne dispose pas de cette compétence actuellement. Pourtant, même si la directive 95/46 ne l'impose pas, la majorité des autorités européennes en sont déjà pourvues[2130]. Cette question retient notre attention car la proposition de loi visant à modifier la loi du 8 décembre 1992[2131] ainsi que la proposition de règlement européen sur la protection des données[2132] confient un pouvoir d'amende à l'autorité de protection des données. Serait-il judicieux que la CPVP puisse imposer des amendes aux administrations qui méconnaîtraient les règles de protection des données ?

> La proposition de loi visant à modifier la loi du 8 décembre 1992 part du constat que « la force d'une législation dépend du contrôle de son respect », et qu' « en Belgique, contrairement à nos pays voisins, la législation relative à la vie privée n'a toujours pas de 'chien de garde' qui puisse intervenir rapidement en cas d'utilisation inappropriée de données à caractère personnel »[2133]. L'octroi, à la CPVP, du pouvoir d'infliger des amendes administra-

[2130] Selon un rapport de l'Agence des droits fondamentaux de l'Union européenne, seules l'autorité de protection des données belge, lituanienne, luxembourgeoise, autrichienne, polonaise, suédoise et anglaise ne disposent pas d'un tel pouvoir (European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II, précité*, p. 34).

[2131] Art. 13 de la proposition de loi du 26 mai 2011 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information, *op. cit.*, n° 53-1509/001, p. 1.

[2132] Art. 79 et s. de la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personne physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final.

[2133] Proposition de loi du 26 mai 2011 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit

> tives est une solution qui « permettrait à l'autorité précitée de réagir avec célérité aux évolutions technologiques rapides. Le risque de se voir infliger une amende administrative jouera un rôle effectif de sensibilisation et de correction »[2134].
>
> Les articles 79 et suivants de la proposition de règlement européen sur la protection des données octroient un pouvoir d'amende aux autorités de protection des données et en fixent le montant maximal par type d'infraction[2135].

593.- Discussion. L'octroi d'un pouvoir d'amende à la CPVP s'envisage avec une acuité particulière dans l'e-gouvernement. Des arguments freinent l'octroi d'une telle prérogative tandis que d'autres, au contraire, l'encouragent.

a) Des hésitations. D'un côté, la prudence est de mise. Si la CPVP inflige une sanction financière à une administration, cela revient, pour l'État, à s'attaquer lui-même ou, pour le dire autrement, à *s'auto-condamner*. En effet, la CPVP n'a pas de personnalité juridique propre. Elle est un organe de l'État. Elle est même un organe du pouvoir exécutif si on admet sa qualité d'autorité administrative[2136]. Dès lors, en infligeant une amende à une administration, la CPVP, organe de l'État, attaquerait un autre organe de l'État. Plus encore, si on admet que la CPVP est organe du pouvoir exécutif, l'amende imposée par cette autorité à une administration est une sanction que le pouvoir exécutif s'infligerait à lui-même. L'argument de l'auto-condamnation de l'État, voire du pouvoir exécutif, fait-il obstacle à l'octroi d'un pouvoir d'amende à la CPVP ?

Pour répondre à cette question, on peut se référer aux réflexions développées par la doctrine au sujet d'une autre problématique juridique, celle de la responsabilité pénale des personnes morales[2137]. L'argument de

---

de consultation et les conseillers en sécurité de l'information, *op. cit.,* n° 53-1509/001, p. 1.

[2134] *Ibid*., p. 7.

[2135] Sans entrer dans une analysée détaillée de ces dispositions, remarquons que les règles relatives au pouvoir d'amende de l'autorité de protection des données sont placées dans l'article 79 consacré aux « sanctions administratives ». Or, les sanctions administratives sont diverses et ne se réduisent pas à l'amende administrative. De plus, la proposition de règlement fixe des maxima d'amendes administratives mais pas de minima. Il n'est donc pas certain que, si la proposition de règlement est adoptée telle quelle, la CPVP soit obligée d'imposer des amendes administratives en cas d'infraction aux règles de protection des données.

[2136] À ce sujet voy. *supra,* n° 575.- et s.

[2137] À ce sujet, voy. not. H. Van Driessche, « Evolutie naar strafrechtelijke (milieu-) aansprakelijkheid van alle publiekrechtelijke rechtspersonen ? », *R.W.,* 1999-2000, pp. 833 à 843 ; J. Messine, « Propos provisoires sur un texte curieux : la loi du 4 mai 1999 instituant la responsabilité pénale des personnes morales », *Rev. Dr. Pén.,* 2000, pp. 644 à 646 ; T. De Gendt, *De strafrechtelijke aansprakelijkheid van burgemeesters en schepenen na de wet van 4 mei 1999. Kunnen burgemeesters en schepenen nog steeds beklaagd€ worden ?,* Brugge, die

l'auto-condamnation de l'État y est invoqué pour justifier l'immunité de responsabilité pénale dont bénéficie notamment l'État[2138] : la condamnation pénale de l'État par un juge reviendrait, pour l'État, à s'attaquer lui-même, ce que l'on ne peut accepter[2139]. Cet argument de l'auto-condamnation est critiqué en doctrine au motif qu'« à la lumière de l'article 33 de la Constitution, ce n'est pas à proprement parler l'État qui poursuit, mais bien l'organe désigné par la Constitution, en l'occurrence le pouvoir judiciaire »[2140], et que, d'ailleurs, l'État peut être condamné civilement. À notre sens, cette critique adressée à l'argument de l'auto-condamnation en matière de responsabilité pénale de l'État ne vaut pas à l'égard du pouvoir d'amende de la CPVP, et ce, pour deux raisons. D'une part, l'amende est infligée par la CPVP elle-même, et non par un juge. On ne peut donc pas dire que, dans le cas de la CPVP, c'est le pouvoir judiciaire qui condamne le pouvoir exécutif. D'autre part, à la différence du juge pénal, la CPVP peut intervenir d'initiative, sans nécessairement être saisie par un citoyen. En d'autres termes, dans l'exercice du pouvoir d'amende, la CPVP tout à la fois initie la poursuite de l'administration, poursuit cette dernière et lui inflige la sanction. Il s'agit donc bien d'une auto-condamnation de l'État voire, d'une auto-condamnation du pouvoir exécutif si on admet que la CPVP est un organe du pouvoir exécutif. En l'occurrence, l'idée que le pouvoir exécutif s'auto-condamne pourrait donc paraître symboliquement assez étrange, plus encore que ne l'est la condamnation de l'État par un juge.

Néanmoins, deux constats poussent à ne pas donner trop de poids à l'argument de l'auto-condamnation.

Premièrement, il n'existe aucune règle constitutionnelle ou légale qui s'opposerait à pareille auto-condamnation. Au contraire, la directive 95/46 dote déjà la CPVP de certains moyens d'action qui, s'ils sont exercés dans l'e-gouvernement, s'assimilent à une auto-condamnation de l'État. Ainsi qu'on l'a dit, la CPVP devrait avoir le pouvoir, notamment, d'enjoindre

---

Keure, 2001, pp. 26 à 46 ; A. De Nauw et F. Deruyck, « De strafrechtelijke verantwoordelijkheid van rechtspersonen », *R.W.,* 1999-2000, pp. 897 à 914 ; M. Nihoul, « L'immunité pénale des collectivités publiques est-elle 'constitutionnellement correcte' ? », *Rev. Dr. Pén.,* 2003, pp. 799 à 839 ; X, *La responsabilité pénale des personnes morales en* Belgique (dir. M. Nihoul), Bruxelles, La Charte, 2005 ; A. Masset, « La responsabilité pénale des personnes orales », *Droit Pén. Entr.,* 2011, pp. 4 et 5 ; P. Waeterinckx, *De strafrechtelijke verantwoordelijkheid van de rechtspersoon en zijn leidinggevenden. Een analyse vanuit de rechts – en bedrijfspraktijk*, Anvers, Intersentia, 2011.

[2138] En vertu de l'article 5 du Code pénal, l'État bénéficie d'une immunité de responsabilité pénale. Un juge ne peut donc pas infliger une sanction pénale à l'État.

[2139] Voy. not. T. De Gendt, *op. cit.,* p. 33 ; H. Van Driessche, *op. cit.,* pp. 839 et 840.

[2140] M. Nihoul, « L'immunité pénale des collectivités publiques est-elle 'constitutionnellement correcte' ? », *op. cit.,* p. 828 et références citées.

au responsable de traitement de faire cesser les traitements de données illégaux[2141]. Si une telle injonction est imposée à une administration, il s'agit d'une sanction que la CPVP impose à l'État qui peut être qualifiée d'auto-condamnation de l'État. Doter la CPVP d'un pouvoir d'amende ne serait qu'une manière de compléter l'arsenal de sanctions que la directive 95/46 lui octroie déjà.

Deuxièmement, le malaise engendré doit être relativisé, en constatant que l'auto-condamnation de l'État et même, l'auto-condamnation du pouvoir exécutif, est déjà pratiquée dans l'administration belge. En effet, le SPF Emploi et, plus particulièrement, la Direction des amendes administrative constituée au sein de ce SPF, peut imposer des amendes administratives pour sanctionner la violation de certaines obligations du droit du travail, comme le prévoit le Code pénal social[2142]. De telles amendes peuvent être imposées aux autorités publiques, puisqu'aucune disposition du Code pénal social ne l'en empêche. D'ailleurs, après discussion avec un membre de la Direction des amendes administratives, il s'avère que des amendes administratives ont déjà été infligées à des communes, au SPF Justice et même au SPF Emploi pour violation de dispositions légales tombant dans le champ de compétence de la Direction des amendes administratives.

> Plus précisément, la procédure suivie par la Direction des amendes administratives varie selon l'importance de l'infraction. Selon la gravité de l'infraction, l'auditeur du travail doit, ou non, intervenir et l'amende administrative est, ou non, une sanction subsidiaire par rapport à la sanction pénale. Par exemple, un service public fédéral a fait travailler un ressortissant étranger qui n'est pas autorisé à séjourner plus de 3 mois en Belgique ni à s'y établir. Cette infraction est punie par l'article 175, §1er du Code pénal social d'une sanction de niveau 4, c'est-à-dire, le niveau le plus sévère de sanctions. Un inspecteur social constate l'infraction commise par le SPF en question et dresse un procès-verbal. Il envoie ensuite ce procès-verbal à l'auditeur du travail et à la direction des amendes administratives du SPF Emploi. Dans un premier temps, il revient à l'auditeur du travail de traiter le procès-verbal. Celui-ci peut soit poursuivre pénalement (proposer une transaction ou poursuivre l'autorité devant le tribunal correctionnel), soit renoncer aux poursuites pénales. Dans cette dernière hypothèse, la direction des amendes

[2141] Voy. *supra,* n° 551.-

[2142] Voy. la loi du 6 juin 2010 introduisant un Code pénal social, *M.B.,* 1er juillet 2010 et, en particulier, le titre 4 du Code pénal social. Des amendes administratives pouvaient déjà être infligées avant l'entrée en vigueur du Code pénal social, en vertu de la loi du 30 juin 1971 relative aux amendes administratives applicables en cas d'infraction à certaines lois sociales, *M.B.,* 13 juillet 1971. Cette loi a été abrogée par la loi du 6 juin 2010 précitée.

administratives peut traiter le procès-verbal et décider de l'application ou non d'une amende administrative.

D'autres infractions sont punies d'une sanction de niveau 1, constituée d'une amende administrative. Il s'agit des infractions les moins graves, telles que des infractions purement administratives, comme le fait de ne pas avoir indiqué une certaine mention dans un certain document. Dans ce cas, l'auditeur du travail n'est pas compétent. Seule l'administration l'est. L'amende administrative est alors une sanction autonome, et non plus une sanction subsidiaire à la sanction pénale.

Outre l'argument de l'auto-condamnation, le fait que l'amende administrative consiste en un *montant financier* incite également à la réflexion. En effet, l'administration, contrainte de payer une amende, verrait son crédit de fonctionnement amputé du montant de cette sanction financière. Cet argent ne pourrait dès lors pas être investi dans les politiques menées par ladite administration, ce qui pourrait nuire à la continuité et à la qualité du service public, au détriment des citoyens. Il faut pourtant éviter que ces derniers pâtissent du paiement de l'amende, car ils auraient déjà eu à subir l'usage abusif des données commis par l'administration sanctionnée et ayant entraîné une violation de leur vie privée[2143].

Cet argument n'empêche pas d'octroyer un pouvoir d'amende à la CPVP. Il convainc seulement de ne pas fixer un montant d'amende à ce point élevé qu'il affecterait le bon déroulement du service public[2144].

b) De l'enthousiasme. En revanche, au-delà de l'argument de l'auto-condamnation et de la nature financière de la sanction, l'idée de doter la CPVP d'un pouvoir d'amende est très intéressante. À n'en pas douter, l'amende agit *préventivement*. On peut raisonnablement penser qu'elle a un effet dissuasif sur les administrations qui ne souhaitent pas voir leur réputation atteinte par une sanction de la part de la CPVP. La menace d'une sanction financière devrait donc inciter le Ministre, le directeur de l'administration concernée et les agents à être attentifs au respect des règles de protection des données. Cette vertu de l'amende administrative est non négligeable dans l'e-gouvernement car il est particulièrement important que les administrations soient dissuadées de violer la protection des données. En effet, rappelons-le, les citoyens sont contraints de livrer leurs informations personnelles aux institutions publiques[2145]. Pourtant, les moyens juridiques à disposition de ces derniers ne leur permettent

[2143] M. Nihoul, « L'immunité pénale des collectivités publiques est-elle 'constitutionnellement correcte' ? », *op. cit.*, pp. 830, 831 et 834 et références citées ; T. De Gendt, *op. cit.*, p. 35.

[2144] Voy. *infra*, n° 594.-

[2145] Voy. *supra*, n° 62.-

pas, actuellement, de contrôler les traitements de données de manière satisfaisante[2146]. Il convient donc de doter la CPVP de moyens d'action efficaces. L'amende administrative répond à ce souci.

L'amende administrative présente également l'intérêt de pouvoir être infligée *directement* à l'administration par la CPVP, sans passer par le ministre responsable[2147], ce qui est appréciable en termes d'efficacité et de rapidité.

En outre, le pouvoir d'amende pourrait *renforcer* utilement les autres sanctions administratives que peut imposer la CPVP. Cette dernière pourrait ainsi menacer les administrations d'une sanction financière si, par exemple, elles ne respectent pas les décisions des comités sectoriels, ou si elles continuent à traiter des données alors que la CPVP leur a enjoint d'arrêter ces agissements[2148].

Enfin, les amendes imposées par la CPVP pourraient contribuer au *financement* de la CPVP. Le produit de l'amende aurait dès lors une affectation particulière et clairement identifiée, à savoir, le financement de notre autorité de protection des données.

594.- L'octroi et l'organisation du pouvoir d'amende. Finalement, serait-il judicieux de conférer un pouvoir d'amende à la CPVP ? Aux termes des développements qui précèdent, il apparaît que l'octroi d'une telle compétence à la CPVP serait bénéfique pour l'efficacité de son action en faveur de la protection de la vie privée des citoyens, tout en ne se heurtant pas à des règles constitutionnelles ou légales. Dès lors, il nous semble judicieux de doter la CPVP d'un pouvoir d'amende qu'elle pourrait exercer à l'égard des administrations.

Il reste à définir les modalités d'exercice de cette prérogative. En particulier, il faut déterminer le montant de l'amende que la CPVP pourrait imposer à une administration qui violerait la protection des données. Comme l'indique la proposition de règlement européen sur la protection des données, ce montant devrait être fixé « en fonction de la situation spécifique, compte dûment tenu, notamment, de la nature, de la gravité et de la durée de l'infraction »[2149].

[2146] Voy. *supra,* n° 469.- et s.

[2147] À la différence du pouvoir de dénonciation dont il a été question plus haut. Voy. *supra,* n° 588.-

[2148] Dans l'hypothèse où, conformément à la directive 95/46, la CPVP dispose d'un pouvoir de faire cesser les traitements de données illégaux. Voy. *supra,* n° 551.-

[2149] Considérant 120 de la proposition de règlement européen sur la protection des données.

Quoi qu'il en soit, le montant de l'amende doit être suffisamment élevé pour être dissuasif, puisque, comme nous l'avons indiqué, il importe que la sanction financière agisse de manière préventive, en incitant l'administration à respecter les règles de protection des données. D'autre part, le montant de l'amende ne doit pas être trop élevé, afin de ne pas porter inutilement atteinte à la continuité et la qualité des services publics. Il en va d'autant plus ainsi que la CPVP pourrait renforcer la sanction qu'elle impose à l'administration en combinant l'amende administrative avec d'autres sanctions.

> Par exemple, elle pourrait infliger une sanction financière à une administration tout en dénonçant celle-ci à la Chambre des représentants pour qu'elle interroge le ministre concerné.

À cet égard, les montants maxima de l'amende administrative tels qu'ils sont fixés par la proposition de règlement européen sur la protection des données semblent si exorbitants qu'ils risquent de nuire fortement à l'action administrative s'ils sont appliqués en pratique.

> Par exemple, la proposition de règlement européen prévoit que l'autorité de protection des données peut infliger une amende s'élevant à 500.000 euros « à quiconque, de propos délibéré ou par négligence [...] fournit des informations incomplètes à la personne concernées »[2150] qui demande l'accès aux informations la concernant.
>
> L'amende peut s'élever à 1.000.000 d'euros si « quiconque, de propos délibéré ou par négligence [...] traite des données à caractère personnel sans base juridique ou sans base juridique suffisante à cette fin »[2151]. Comment un agent de l'administration peut-il apprécier si, concrètement, la base juridique est « suffisante » ? Cette question est d'autant plus difficile que, comme en atteste le premier titre de la recherche, le législateur semble lui-même éprouver des difficultés à rédiger des normes de qualité pour encadrer l'e-gouvernement.

En revanche, on pourrait s'inspirer des montants des amendes que peut imposer la Direction des amendes administratives pour sanctionner les infractions reprises dans le livre 2 du Code pénal social. Ces montants ne diffèrent pas selon que l'employeur est une autorité publique ou non. Ils semblent tout de même plus raisonnables que les montants fixés par la proposition de règlement européen en matière de protection des données.

[2150] Art. 79.5 de la proposition de règlement européen sur la protection des données.
[2151] *Ibid.,* art. 79.6.

> Ces montants sont repris à l'article 101 du Code pénal social qui dispose que « les infractions visées au Livre 2 sont punies d'une sanction de niveau 1, de niveau 2, de niveau 3 ou de niveau 4.
>
> La sanction de niveau 1 est constituée d'une amende administrative de 10 à 100 euros[2152].
>
> La sanction de niveau 2 est constituée soit d'une amende pénale de 50 à 500 euros, soit d'une amende administrative de 25 à 250 euros.
>
> La sanction de niveau 3 est constituée soit d'une amende pénale de 100 à 1000 euros, soit d'une amende administrative de 50 à 500 euros.
>
> La sanction de niveau 4 est constituée soit d'un emprisonnement de six mois à trois ans et d'une amende pénale de 600 à 6000 euros ou de l'une de ces peines seulement, soit d'une amende administrative de 300 à 3000 euros »[2153].

Le montant des amendes administratives que la CREG peut infliger pourrait également inspirer le législateur pour encadrer le pouvoir d'amende de la CPVP. La loi du 29 avril 1999 dispose que « l'amende ne peut être, par jour calendrier, inférieure à mille deux cent quarante euros ni supérieure à cent mille euros, ni, au total, supérieure à deux millions d'euros »[2154].

> Par exemple, dans une affaire mentionnée précédemment[2155], en 2004, la CREG a infligé à la Ville de Wavre une amende est de 1239.46 euros par jour calendrier[2156]. Remarquons que ce montant est situé dans le bas de l'échelle des amendes que la CREG peut imposer, ce qui pourrait peut-être être un élément qui conforte l'idée selon laquelle le montant de l'amende doit être modéré lorsque l'autorité condamnée est une institution publique.

[2152] C'est nous qui soulignons.

[2153] Précisons qu'en vertu de l'article 102 du Code pénal social, le montant des amendes pénales et des amendes administratives sont soumis aux décimes additionnels. Concrètement, les montants indiqués doivent donc être multipliés par un coefficient multiplicateur et actuellement il est de 6.

[2154] Art. 31 de la loi du 29 avril 1999 précitée.

[2155] Voy. *supra*, n° 515.-

[2156] Décision de la CREG (B) 040506-CDC-294 du 6 mai 2004. À l'époque, l'article 31 de la loi du 29 avril 1999 prévoyait que « l'amende ne peut être, par jour calendrier, *in*férieure à cinquante mille francs ni supérieure à quatre millions de francs, ni, au total, supérieure à quatre-vingts millions de francs ».

C. La capacité de saisir la Cour constitutionnelle et le Conseil d'État

595.- L'octroi de la personnalité juridique à la CPVP. Ainsi qu'on l'a dit[2157], l'e-gouvernement est encadré par de nombreuses normes de valeur législative et de valeur réglementaire. Certaines de ces normes sont sujettes à critique en ce qui concerne leur constitutionnalité et leur légalité au regard du régime juridique de la protection des données.

À cet égard, on a souligné l'intérêt des recours devant la Cour constitutionnelle et la section du contentieux administratif du Conseil d'État, qui permettent notamment d'obtenir l'annulation des normes attaquées[2158]. Malheureusement, pour l'heure, ces recours manquent d'effectivité, étant rarement mis en œuvre par les citoyens[2159].

Dans ce contexte, il serait judicieux de permettre à la CPVP d'agir elle-même à la Cour constitutionnelle et au Conseil d'État, pour contester les normes qui portent atteinte au régime juridique de la protection des données à caractère personnel. D'ailleurs, selon un rapport de l'Agence des droits fondamentaux de l'Union européenne (FRA), une telle capacité d'ester en justice est d'ailleurs présentée comme un moyen de renforcer l'indépendance de l'autorité de protection des données[2160].

Pour ce faire, il est nécessaire d'octroyer la personnalité juridique à la CPVP. En effet, outre les autorités gouvernementales et les autorités parlementaires, seule une « personne physique ou morale justifiant d'un intérêt »[2161] peut introduire un recours en annulation et/ou en suspension devant la Cour constitutionnelle. L'octroi de la personnalité morale à la CPVP est donc une condition nécessaire pour qu'elle puisse intenter pareil recours.

> Par exemple, la CREG, autorité de régulation disposant de la personnalité juridique, peut agir à la Cour constitutionnelle[2162].

Dans le même sens, seuls les organismes dotés de la personnalité juridique sont aptes à introduire un recours au Conseil d'État[2163].

2157 Voy. *supra,* Titre I.

2158 Voy. *supra,* n° 432.- et s.

2159 Voy. not. *supra,* n° 434.-

2160 Rapport European Union Agency for fundamental rights, Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II, précité, pp. 20 et 47.

2161 Art. 2, 2°, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle.

2162 Voy. C.C., arrêt n° 84/2010 du 8 juillet 2010.

2163 M. Leroy, *Contentieux administratif, op. cit.*, p. 483.

D. La suppression des comités sectoriels

596.- De nombreuses difficultés. Pour l'heure, rappelons-le, les comités sectoriels institués au sein de la CPVP disposent d'un important pouvoir de décision : celui d'autoriser ou d'interdire le traitement des données enregistrées dans certaines bases de données de l'administration.

L'existence de ces comités sectoriels soulève des difficultés. La présente recherche a montré, tout d'abord, que leur indépendance n'est pas garantie. On a également souligné qu'il n'est pas certain que les décisions des comités sectoriels puissent être attaquées au Conseil d'État, section du contentieux de l'administration. C'est pourquoi, à l'occasion des réflexions sur le statut de la CPVP, on a proposé de faire de celle-ci une autorité administrative indépendante, en renforçant les garanties d'indépendance et en assurant notamment le contrôle juridictionnel de cette autorité. Ce faisant, les décisions des comités sectoriels pourraient être attaquées en justice.

Néanmoins, même si de telles modifications étaient effectuées, on ne peut ignorer les critiques plus concrètes. Les administrations se plaignent de la lourdeur de la procédure à suivre, qui ralentit l'exécution de leurs missions. Les citoyens souffrent de l'obscurité des règles appliquées et du manque d'uniformité des décisions rendues. Il y a également fort à parier que l'existence de ces autorités qui se multiplient et sont composées de nombreux membres soit financièrement lourde. Face à ces difficultés, ne pourrait-on pas se passer des comités sectoriels ?

§1. La nécessité d'un changement

597.- L'évolution du contexte. Rappelons[2164] que l'ancêtre des comités sectoriels est le comité de surveillance de la Banque-Carrefour de la sécurité sociale. Cette institution a été créée pour autoriser la communication de « données sociales à caractère personnel » « par les institutions de sécurité sociale »[2165]. En d'autres termes, cette procédure d'autorisation ne pesait que sur un nombre restreint d'administrations, pour un nombre restreint de données et en n'appliquant qu'une seule loi, celle du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale.

Aujourd'hui, la lourdeur de la procédure d'autorisation affecte quasiment l'ensemble de l'administration : la plupart des institutions publiques

[2164] Voy. *supra,* n° 537.-

[2165] Art. 15 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, dans sa version initiale, *Pasin.,* I, 1990, p. 58.

traitent des données à caractère personnel, et la plupart de ces données sont soumises à une obligation d'autorisation de comité sectoriel. En outre, les décisions des comités sectoriels se sont complexifiées au point qu'elles sont peu prévisibles. Cela est lié, d'une part, au fait que l'arsenal normatif s'est considérablement amplifié. Il ne s'agit plus seulement d'appliquer la loi du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale. D'autres normes sont à prendre en compte, telles que la loi du 8 décembre 1992 et les législations particulières s'appliquant à certains types de données. D'autre part, les questions juridiques traitées évoluent au gré des technologies, si bien que certaines problématiques nécessitent de réelles compétences informatiques pour les appréhender. On pense, par exemple, à la compréhension du fonctionnement d'un entrepôt de données, dit aussi « *datawarehouse* ». Enfin, le nombre de comités sectoriels s'est multiplié, générant notamment des questions relatives à la détermination du comité sectoriel compétent.

La procédure d'autorisation par les comités sectoriels est donc devenue trop lourde et trop complexe. Partant de ce constat, il s'impose de réfléchir à la nécessité de maintenir leur existence aujourd'hui.

§2. Les ententes de partage

598.- Le besoin de régulation. De toute évidence, ainsi qu'on l'a déjà dit[2166], le législateur et le Gouvernement ne peuvent envisager ni anticiper, dans les normes applicables à l'e-gouvernement, la multitude de traitements de données effectués au sein de l'administration. Partant de ce constat, il s'impose de mettre en place un relais qui, sur le terrain et au cas par cas, veillera au respect des normes. Les comités sectoriels répondent à ce besoin, en rendant des décisions au cas par cas, qui complètent l'arsenal normatif dans le secteur des traitements de données à caractère personnel. Leurs décisions contribuent donc à assurer la régulation de ce secteur.

Ce besoin de régulation ne peut être nié et doit recevoir toute notre attention. Toutefois, à notre sens, il pourrait être satisfait en se passant des comités sectoriels.

599.- Une solution canadienne. Comme on l'a évoqué dans le premier titre de la recherche[2167], une solution pourrait être envisagée qui responsabilise davantage les administrations, tout en maintenant un contrôle assuré par la CPVP. Il s'agit de l'édification d' « ententes de partage »,

[2166] Voy. *supra,* n° 490.- et s.
[2167] Voy. *supra,* n° 222.- et s.

solution en vigueur au Canada. La solution proposée dans les lignes qui suivent est directement inspirée de celle qui s'applique aux organismes publics du Québec et qui est organisée par la loi québecquoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[2168].

600.- Deux postulats de départ. Deux postulats président aux développements qui suivent.

D'une part, d'ici peu, chaque administration disposera de son propre détaché à la protection des données, puisque telle est l'obligation qui sera prochainement imposée par le nouveau règlement sur la protection des données[2169].

D'autre part, il faut admettre que l'exigence de transparence, consacrée par l'article 32 de la Constitution, impose de dresser le panorama des administrations existantes et des sources authentiques détenues au sein de chacune d'elle[2170]. De cette manière, chaque citoyen, mais aussi chaque administration, sera en mesure de savoir « qui a quoi ».

601.- La conclusion des ententes de partage. Partant de là, le contrôle des échanges de données au sein de l'administration pourrait se faire en trois étapes, que l'on décrit de suite.

a) Première étape. Lorsqu'une administration, dite « administration demanderesse », a besoin d'informations qu'elle ne détient pas, son détaché à la protection des données serait chargé d'identifier la source authentique contenant les données recherchées. Il contacterait ensuite le détaché à la protection des données de l'administration responsable de cette source authentique, appelée « administration émettrice ». Le détaché à la protection des données de l'administration demanderesse et le détaché à la protection des données de l'administration émettrice évalueraient ensemble les conditions auxquelles le transfert de données envisagé pourrait légalement être effectué. Ils concluraient ensuite une « entente de partage » reprenant ces conditions.

À ce stade, le principal travail de réflexion juridique serait ainsi effectué par les détachés à la protection des données des administrations concernées. Ce faisant, un premier contrôle du transfert de données envisagé serait réalisé par les détachés à la protection des données.

[2168] Voy. les art. 68 et 70 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Québec).

[2169] Voy., *supra*, n° 552.- et s.

[2170] Voy. *supra,* n° 377.- et s.

Par exemple, l'article 68 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels exige que les indications suivantes soient reprises dans l'entente de partage :

« 1° l'identification de l'organisme public qui communique le renseignement et celle de la personne ou de l'organisme qui le recueille ;

2° les fins pour lesquelles le renseignement est communiqué ;

3° la nature du renseignement communiqué ;

4° le mode de communication utilisé ;

5° les mesures de sécurité propres à assurer la protection du renseignement personnel ;

6° la périodicité de la communication ;

7° la durée de l'entente ».

b) Deuxième étape. Dans le premier titre de la recherche, nous avons encouragé la mise en place d'un e-gouvernement en réseaux, fondé notamment sur l'utilisation de plateformes d'échanges d'informations. Celles-ci formeraient le cœur d'un réseau sectoriel et seraient chargées d'acheminer les données vers l'administration qui les a demandées. Dès lors, comme nous l'avons déjà suggéré[2171], une fois l'entente de partage rédigée, il conviendrait de la transmettre à la plateforme d'échanges d'informations. Celle-ci devrait s'y référer au moment d'acheminer les données demandées à l'administration demanderesse.

Un deuxième contrôle des données pourrait ainsi être réalisé puisque, concrètement, la plateforme veillerait à ne transmettre effectivement que les données entérinées dans l'entente de partage.

c) Troisième étape. Il conviendrait de placer cette entente sous la surveillance de la CPVP, de manière à ce qu'elle soit en mesure de vérifier la légalité de l'échange de données et d'assurer sa transparence[2172]. De cette manière, un troisième contrôle est assuré par la CPVP, si elle décide d'étudier la légalité de l'entente de partage et d'investiguer davantage si elle le souhaite. Un quatrième contrôle peut également être effectué par les citoyens qui, grâce aux mesures de transparence, ont connaissance des échanges de données entre les administrations.

Comment faire en pratique ? Pour les échanges de données effectués au sein d'un réseau sectoriel, on pourrait prévoir que l'entente est transmise à la CPVP, de manière à ce que celle-ci puisse exercer un contrôle *a posteriori* de l'échange et effectuer les mesures de publicité nécessaires.

[2171] Voy. *supra,* n° 223.-
[2172] Voy. *supra,* n° 224.-

Si l'échange de données a lieu entre deux réseaux sectoriels distincts, la CPVP pourrait être chargée d'analyser l'entente de partage et de rendre un avis endéans un délai raisonnable. Si l'avis de la CPVP est favorable, l'échange de données peut être effectué. En cas d'avis défavorable de la CPVP, la collecte indirecte de données ne peut être réalisée.

> Au Québec, la Commission d'accès à l'information doit rendre son avis dans les 60 jours suivant la réception de la demande d'avis accompagnée de la copie de l'entente de partage.
>
> Dans cet avis, la Commission d'accès à l'information doit prendre en considération :
>
> « 1° la conformité de l'entente aux conditions visées à l'article 68 [...] ;
>
> 2° l'impact de la communication du renseignement sur la vie privée de la personne concernée, le cas échéant, par rapport à la nécessité du renseignement pour l'organisme ou la personne qui en reçoit communication ».

Les avis de la CPVP et les ententes de partage devraient être publiés sur le site de la CPVP, afin de garantir leur transparence. Ils pourraient également être utilisés par la CPVP pour constituer le cadastre des interconnexions, outil de transparence dont il a été question dans le deuxième titre de la présente recherche[2173].

> Au Québec, les ententes de partage, accompagnés de avis de la Commission d'accès à l'information, sont publiés sur le site internet de cette dernière, dans une rubrique « avis administratifs sur les ententes de communication »[2174].

602.- Appréciation de ce mécanisme. Certes, la solution des ententes de partage présente une certaine lourdeur, dans la mesure où les administrations doivent rédiger une entente de partage et attendre l'autorisation de la CPVP dans l'hypothèse d'un échange de données inter-réseaux. Néanmoins, elle présente beaucoup d'avantages.

Tout d'abord, cette lourdeur doit être *relativisée*. On peut raisonnablement penser que cette procédure serait plus légère que celle qui impose de passer par un comité sectoriel. En effet, les détachés à la protection des données connaissent leur administration et les règles applicables aux échanges de données entre administrations. Ils peuvent identifier précisément les informations dont leur administration a réellement besoin, afin de respecter l'exigence de proportionnalité, tout en ciblant au mieux la finalité du traitement et vérifier que celle-ci entre dans les missions de

---

[2173] Voy. *supra*, n° 392.-

[2174] Voy. http://www.cai.gouv.qc.ca/decisions-et-avis/section-surveillance/avis-administratifs/#Ententes

l'administration concernée. Par la suite, une fois les règles de fond fixées dans l'entente de partage grâce aux analyses menées par les détachés à la protection des données, l'intervention de la CPVP sera d'autant plus allégée.

Ensuite, ces ententes ont le mérite de la *clarté* et de la *transparence*. Elles fixent des règles et des responsabilités qui sont en principe bien comprises par les administrations partenaires. Elles n'en seront que mieux appliquées. De plus, ces ententes sont publiées, sur le site de la CPVP et peuvent servir à constituer le cadastre des interconnexions. Elles servent donc l'objectif de transparence et facilitent le contrôle, par les citoyens, de tels échanges[2175].

Enfin, cette manière de procéder aurait également une *portée symbolique*. Elle placerait les administrations dans un rôle d'acteur de la protection des données. Ce régime juridique pourrait alors être perçu davantage comme un idéal à atteindre, plutôt qu'un arsenal normatif contraignant supplémentaire.

*

Conclusions

Dans ce troisième chapitre, nous avons étudié la manière d'améliorer le contrôle de l'e-gouvernement grâce à la CPVP, autorité de régulation dans le secteur des traitements de données à caractère personnel. Plus particulièrement, nous nous sommes penchés sur les améliorations qui peuvent être apportées au statut de la CPVP et aux moyens d'actions dont cette autorité dispose.

Le statut de la CPVP doit être clarifié. Son indépendance doit être renforcée. Toutefois, cette autorité de régulation ne peut pour autant agir dans l'ombre. Elle dispose de multiples prérogatives, parmi lesquelles un pouvoir de décision exercé par ses comités sectoriels. Il faut qu'elle assume la responsabilité de ses actes et que, le cas échéant, les manquements graves de ses membres soient sanctionnés. C'est pourquoi, des pistes ont été proposées, qui tentent de définir les contours du délicat équilibre à trouver entre deux exigences *a priori* contradictoires : l'indépendance et le contrôle.

Par ailleurs, le contrôle de l'e-gouvernement gagnerait à voir les prérogatives de la CPVP renforcées et adaptées aux particularités du secteur

[2175] Voy. *supra,* n° 224.-

public. Des moyens d'action peuvent lui être octroyés, qui assurent davantage d'efficacité aux décisions qu'elle impose à l'administration. À cet égard, un pouvoir d'injonction, un pouvoir d'admonestation et un pouvoir d'amende devraient être définis. La personnalité juridique devrait lui être reconnue, de manière à ce que la CPVP puisse agir devant la Cour constitutionnelle et le Conseil d'État. Son pouvoir de dénonciation devrait être plus souvent exercé. En outre, la CPVP devrait faire davantage œuvre de pédagogie, en veillant à la clarté et la lisibilité des documents qu'elle émet, qu'il s'agisse de ses décisions, de ses avis ou de ses recommandations. Cela contribuerait utilement à la diffusion des règles de protection des données dans la société en général. Enfin, la nécessité des comités sectoriels est remise en cause. Une solution alternative existe, qui consiste en l'édification d' « ententes de partage » et qui est inspirée d'une solution québécoise. Elle est selon nous, mieux adaptée au besoin de régulation dans le secteur des traitements de données à caractère personnel.

*

Conclusions du Titre III

L'effectivité de la protection de la vie privée des citoyens suppose que l'e-gouvernement soit contrôlé.

Les contrôles organisés par le droit administratif général sont pertinents dans l'e-gouvernement, bien qu'ils aient été organisés avant l'informatisation de l'administration. En particulier, on a souligné l'importance des sanctions qui peuvent être imposées par les juridictions constatant une violation du régime juridique de la protection de la vie privée et des données à caractère personnel. Ainsi, la Cour constitutionnelle peut annuler une norme de valeur législative contraire aux règles nationales et supranationales en cette matière, ou déclarer son inconstitutionnalité suite à une question préjudicielle. Les normes de valeur réglementaire qui méconnaissent ce régime juridique peuvent être annulées par le Conseil d'État. Quant aux juridictions judiciaires, elles peuvent condamner l'administration à réparer le dommage causé par l'usage abusif de données à caractère personnel, en vertu de l'article 1382 du Code civil, ou refuser d'appliquer une norme de valeur réglementaire illégale, en vertu de l'article 159 de la Constitution. Le Médiateur fédéral, la section de législation du Conseil d'État et la CADA assurent également un rôle important dans l'e-gouvernement bien qu'ils ne soient pas compétents pour imposer des sanctions contraignantes. Leurs avis et leurs recommandations éclairent utilement l'interprétation du droit administratif dans le contexte de l'e-gouvernement.

Néanmoins, ces voies de contrôle révèlent des faiblesses dans l'e-gouvernement, tenant notamment au fait que les moyens d'action sont mal adaptés à la rapidité et à la technicité des traitements de données à caractère personnel. On constate aussi que les citoyens n'exercent pas les voies de contrôle qui leur sont offertes. Soit ils ignorent les illégalités commises, soit ils n'ont pas le courage ni les moyens de dénoncer les abus commis dans l'administration.

Partant de ces constats, les moyens de contrôle organisés par le régime juridique de la protection des données gagnent à être étudiés et complètent utilement le droit administratif. En effet, chaque citoyen peut faire valoir certains droits directement à l'égard de l'administration, qui visent spécifiquement à obtenir la correction des erreurs affectant les données voire la cessation des traitements de données illégaux en cours d'exécution. Des actions judiciaires particulières sont également organisées. La recherche a toutefois souligné les embûches auxquelles se heurtent pareilles prérogatives et a proposé des solutions pour améliorer la protection du citoyen.

Par ailleurs, une nouvelle fonction a vocation à apparaître au sein des administrations, celle de détaché à la protection des données. Cet expert de la matière doit veiller à la légalité des traitements de données au sein de l'administration qui l'engage. On regrette que le statut de détaché à la protection des données n'ait pas encore été organisé en Belgique. Néanmoins, il faudra s'y atteler prochainement car la présence de ces personnes sera vraisemblablement obligatoire dès l'entrée en vigueur du règlement européen sur la protection des données à caractère personnel.

Enfin, de longs développements ont été consacrés à la CPVP. Cette autorité de régulation joue un rôle essentiel pour la protection de la vie privée des citoyens, particulièrement dans le contexte de l'e-gouvernement. Elle dispose de moyens d'action lui permettant de prendre le relais du citoyen, en exerçant notamment une action d'intérêt collectif auprès du juge judiciaire. D'autres prérogatives lui offrent la possibilité d'agir de manière souple et rapide. On pense à la procédure de médiation qu'elle privilégie particulièrement dans l'exercice de ses missions. Néanmoins, nous avons montré que le statut de la CPVP pose question. Il est difficile de combiner, d'une part, l'exigence d'indépendance qui s'impose à la CPVP et qui est interprétée de manière large par la Cour de justice de l'Union européenne, et, d'autre part, le contrôle politique de la CPVP exigé par la Constitution et la Cour constitutionnelle. On s'est aussi interrogé sur la qualité d'autorité administrative de la CPVP, de laquelle dépend le contrôle juridictionnel de cette autorité. On a également regretté que la CPVP n'ait pas la personnalité juridique, qui renforcerait son indépendance et sa responsabilité. L'efficacité de l'action de la CPVP a également été mise en doute, en regrettant notamment que la CPVP ne dispose pas d'un pouvoir d'injonction, d'admonestation et d'amende, contrairement à son homologue français, par exemple. Ces importantes questions expliquent que le troisième chapitre ait été entièrement consacré à proposer des pistes de solutions pour clarifier le statut de la CPVP et renforcer l'efficacité de son action.

*

Conclusions générales

Au terme de ces développements, l'hypothèse de la recherche est confirmée : il est possible d'organiser un e-gouvernement à la fois efficace et respectueux de la vie privée des citoyens.

La tâche est délicate. Elle suppose d'identifier clairement les dangers de l'e-gouvernement et d'y répondre adéquatement. La recherche a montré qu'au-delà de l'enthousiasme généré par l'usage des technologies au sein de l'administration, il importe d'être conscient des risques de l'e-gouvernement, le risque majeur étant de provoquer un déséquilibre important entre le pouvoir de l'administration et les prérogatives du citoyen.

Certes, le déséquilibre entre l'administration et le citoyen n'est pas propre à l'utilisation des technologies et il existe depuis longtemps. En effet, le droit administratif est traditionnellement fondé sur l'inégalité entre l'administration « qui doit faire prévaloir l'intérêt général, et [...] l'administré, qui ne défend en général que son intérêt personnel »[2176]. Cette inégalité se traduit notamment par le pouvoir de l'administration de prendre des décisions unilatérales et exécutoires, génératrices d'obligations à charge des administrés[2177]. Organiser une stricte égalité entre les droits et les devoirs de l'administration et du citoyen est d'ailleurs inconcevable, car elle « impliquerait l'abolition de la forme étatique elle-même »[2178]. Néanmoins, l'utilisation des technologies au sein de l'administration risque d'accentuer fortement ce déséquilibre. L'enregistrement des multiples données des citoyens et les outils qui permettent d'exploiter ces informations renforcent la puissance de l'administration. Cette dernière est à présent en mesure d'avoir une connaissance précise de chaque citoyen. Dans le même temps, l'action de l'administration informatisée est plus opaque, compte tenu de la difficulté pour le citoyen de savoir ce que l'administration détient sur lui et de comprendre l'usage qui est fait de ses informations. Dans ce contexte, on peut craindre que l'administration agisse comme un *Big brother* qui surveille chaque individu. Plus

---

[2176] A. Mast, A. Alen et J. Dujardin, *Précis de droit administratif*, Bruxelles, Story-Scientia, 1989, p. 5.

[2177] J. Chevallier, « Le droit administratif, un droit de privilège ? », *Pouvoirs*, 1988, n° 46, p. 60 ; J. Dembour, *Droit administratif*, 3e éd., Faculté de droit, d'économie et de sciences sociales de Liège, 1978, p. 14.

[2178] J. Chevallier, *op. cit.*, p. 67.

fondamentalement, une administration kafkaïenne, distante, incomprise, incontrôlable risque d'émerger.

Il importe donc d'attribuer à chacun les moyens d'exercer une prise sur l'administration, pour la comprendre et la contrôler, notamment en dénonçant les abus éventuels qui la conduiraient à prendre des décisions discriminatoires. En particulier, à l'heure de l'e-gouvernement, la prise du citoyen sur l'administration suppose que soit garanti à chacun le droit à la vie privée entendu dans le sens du droit à l'autodétermination informationnelle. Chacun a le droit de savoir où sont enregistrées ses données, de comprendre l'usage qui en est fait, de contester les utilisations abusives et d'obtenir que l'administration ayant traité illégalement ces données soit condamnée à réparer le dommage causé par l'atteinte au droit fondamental à la vie privée. Ces prérogatives contrebalancent la puissance que l'administration acquiert par les technologies.

Dès lors, pour protéger la vie privée des citoyens dans l'e-gouvernement, il s'impose de modifier en profondeur le droit administratif. Celui-ci doit être modernisé et enrichi grâce aux règles de protection de la vie privée et des données à caractère personnel actuellement en vigueur (I.). Il faut en effet considérer que ces règles font partie intégrante du droit administratif, étant donné que l'organisation et le fonctionnement de l'administration y sont soumis. Elles doivent dès lors être étudiées par les administrativistes, enseignées dans les cours de droit administratif et appliquées par les juridictions. En outre, pour endiguer les dangers de l'e-gouvernement qui existent déjà et risquent de s'amplifier à l'avenir, il convient de dégager des solutions nouvelles, qui renforcent la protection de la vie privée des citoyens dans l'administration. Le législateur, l'autorité de protection des données et la technologie elle-même peuvent y contribuer. Ces solutions conduisent à rééquilibrer la relation entre le citoyen et l'administration dans l'e-gouvernement (II.).

I. L'enrichissement du droit administratif

L'action administrative a gagné en efficacité et en qualité grâce aux traitements de données à caractère personnel sur lesquels elle se fonde largement. Demander à un citoyen qu'il communique une information personnelle, transférer une donnée à une autre administration, prendre une décision administrative en consultant une ou plusieurs bases de données, constituent désormais des actes accomplis quotidiennement par l'administration. Aussi indéniables soient leurs atouts, ces actes en appellent tous au respect du régime juridique de la protection des données. C'est pourquoi, les règles de protection des données applicables à l'administration font aujourd'hui partie intégrante du droit administratif.

Intégrer les règles de protection des données dans le droit administratif n'est pas un exercice aussi artificiel qu'il en a l'air, même si, jusqu'à présent, les publicistes et les spécialistes de la protection des données se sentent appartenir à des mondes étrangers. La présente recherche a visé à démontrer que le régime juridique de la protection des données conforte et même renforce le droit administratif qui s'applique à l'administration de manière générale.

La démonstration a été faite au départ de trois piliers de l'État de droit que sont l'exigence de légalité, l'exigence de transparence et l'exigence de contrôle. Les règles de protection des données peuvent être greffées sur ces exigences. Plus encore, elles doivent l'être, car le régime juridique de la protection des données enrichit la légalité, la transparence et le contrôle de l'administration.

1. Légalité. Les règles de protection des données précisent l'exigence de légalité qui encadre l'action administrative. Les notions de légitimité, de finalité, de précision, de loyauté, de proportionnalité guident le législateur au moment d'organiser l'e-gouvernement. C'est d'autant plus important qu'à l'heure actuelle, la loi est en déclin. Ce constat est dressé dans de nombreux domaines du droit mais paraît particulièrement évident dans l'e-gouvernement, qui est soumis à des lois éparses, lacunaires et difficilement compréhensibles. Dès lors, les règles supranationales de protection des données conduisent le législateur à édicter des lois de meilleure qualité, qui balisent précisément le fonctionnement de l'administration et le font de manière plus compréhensible pour les citoyens.

Nos réflexions sur l'exigence de légalité ont permis notamment de cerner les éléments essentiels des traitements de données qui, en vertu de l'article 22 de la Constitution tel qu'interprété par la Cour constitutionnelle et la section de législation du Conseil d'État, doivent être déterminés par le législateur. Nous avons également montré que le modèle d'État en réseaux dans lequel s'engage l'administration belge depuis quelques années est pleinement justifiable au regard du souci de protéger la vie privée des citoyens. Il conviendrait néanmoins d'organiser un cadre juridique propre à l'e-gouvernement, qui soit plus cohérent et plus compréhensible que les normes actuellement applicables en cette matière. C'est la raison pour laquelle nous avons notamment proposé l'adoption d'une loi-cadre pour l'e-gouvernement et l'adoption de certaines lois particulières.

2. Transparence. À l'heure de l'e-gouvernement, la transparence ne se réduit plus à la divulgation des documents détenus par l'administration et à la motivation de ses décisions. En effet, aujourd'hui, l'administration doit être en mesure de justifier plus précisément son mode de

fonctionnement. Elle doit révéler au citoyen les informations dont elle dispose à son sujet, lui expliquer les raisons pour lesquelles elle conserve ses données, l'informer de l'usage qu'elle en fera ultérieurement, justifier la logique qui sous-tend un traitement de données, etc. Ces prérogatives permettent au citoyen de faire la lumière sur le sort réservé à ses données au sein de l'administration. La prise de l'individu sur l'action administrative est ainsi renforcée puisqu'avant l'entrée en vigueur des règles de protection des données, l'administration n'était pas contrainte de justifier l'usage qu'elle faisait des informations des citoyens. En outre, la publicité active de l'administration est favorisée par le régime juridique de la protection de la vie privée et des données à caractère personnel. L'administration doit, d'initiative, communiquer certaines informations au citoyen qui se voit ainsi épargné de la charge d'effectuer lui-même certaines démarches en matière de transparence.

3. Contrôle. Le régime juridique de la protection de la vie privée et des données à caractère personnel engendre un contrôle plus serré de l'action administrative. D'une part, de nouveaux arguments juridiques peuvent être invoqués devant les juridictions. Ils permettent notamment de contrôler la légalité de certains agissements de l'administration échappant jadis au contrôle du juge. On pense aux transferts de données entre administrations dont la légalité peut à présent être contrôlée même s'il s'agit de mesures préparatoires aux décisions administratives. D'autre part, des recours particuliers sont organisés, qui peuvent s'exercer cumulativement ou non, et qui s'ajoutent aux contrôles organisés par le droit administratif général. On peut les regrouper en trois catégories.

Tout d'abord, le citoyen lui-même peut contrôler l'e-gouvernement, en s'adressant directement à l'administration et en faisant valoir ses droits de rectification, d'interdiction et d'opposition, sans devoir saisir un juge.

Ensuite, le contrôle de l'e-gouvernement peut s'exercer en interne, au sein de l'administration, grâce à une fonction d'un genre nouveau, celle de détaché à la protection des données. Ces spécialistes de la protection des données jouissent d'un statut protégé qui leur assure une indépendance à l'égard de l'administration qu'ils contrôlent. Ce rôle est riche, puisque le détaché à la protection des données peut, non seulement, veiller à la légalité des traitements de données effectués par son administration, mais également aider les agents de l'administration à appliquer cette matière difficile. Il peut aussi être un point de contact utile pour les citoyens et pour la Commission de la protection de la vie privée, notamment. Malheureusement, à l'heure actuelle, le statut de détaché à la protection des données n'est toujours pas organisé en Belgique. Cette lacune devra prendre fin dès l'entrée en vigueur du règlement européen sur la

protection des données à caractère personnel, qui impose la présence d'un détaché à la protection des données dans chaque administration.

Enfin, des contrôles externes s'appliquent également à l'e-gouvernement. Ils sont exercés par la Commission de la protection de la vie privée qui dispose de moyens d'action adaptés à la technicité et à la rapidité des traitements de données à caractère personnel. Le régime juridique de la protection de la vie privée et des données à caractère personnel organise également des recours particuliers devant le juge judiciaire. Ce dernier peut être saisi par le citoyen, qui bénéficie d'une action « comme en référé » devant le président du tribunal de première instance. Elle peut être utilisée pour obtenir du juge qu'il condamne l'administration à respecter certaines obligations légales. Par ailleurs, le juge judiciaire peut également être saisi d'une action d'intérêt collectif initiée par la Commission de la protection de la vie privée.

II. Le rééquilibrage du droit administratif

Désormais, le droit fondamental à la protection de la vie privée irrigue le droit administratif. Le droit administratif en est influencé et doit se construire autour du souci de protéger le citoyen face à une administration de plus en plus puissante. Il convient donc de prolonger le mouvement de « subjectivisation »[2179] du droit administratif qui s'est engagé il y a déjà plusieurs décennies, qui consiste à placer le citoyen au cœur du droit administratif. Un souffle nouveau doit lui être donné dans le contexte de l'e-gouvernement.

Rappelons qu'à l'origine, et pendant des années, l'administration s'apparente à une forteresse, froide, distante et secrète, imposant des décisions unilatérales et exécutoires à des administrés soumis. Dans ce contexte, le droit administratif est « l'expression de la suprématie administrative, l'enveloppe et le vecteur de sa puissance »[2180].

Progressivement, le droit administratif entraîne l'administration dans un mouvement d'*ouverture* envers le citoyen, en organisant notamment des règles de transparence administrative et en créant ainsi les conditions d'un dialogue entre les deux protagonistes[2181]. À cet égard, on a souligné

[2179] J.-B. Auby, « La bataille de San Romano. Réflexions sur les évolutions récentes du droit administratif », *A.J.D.A.*, 2001, p. 917. Voy. égal. p. 195.

[2180] J. Chevallier, « Les fondements du droit administratif à l'épreuve de l'Europe », *in La puissance publique à l'heure européenne* (dir. P. Raimbault), Dalloz, Paris, 2006, p. 39.

[2181] J.-M. Pontier, « Qu'est-ce que le droit administratif ? », *A.J.D.A.*, p. 1939 ; J.-B. Auby, *op. cit.*, p. 917 ; D. De Roy, « La nature des prétentions de l'usager au bénéfice des prestations de service public : essai de typologie », *in Le service public : passé, présent et avenir*

l'importance des législations relatives à la publicité de l'administration et à la motivation formelle des actes administratifs qui permettent au citoyen de prendre place dans la société démocratique en étant pleinement éclairé sur l'environnement administratif qui l'entoure et en comprenant les décisions qui lui sont imposées.

Aujourd'hui, le droit administratif ne doit plus seulement inciter l'administration à s'ouvrir au citoyen. Il doit aussi *protéger* ce dernier contre les abus que l'administration pourrait commettre dans l'utilisation de ses données à caractère personnel. « Désormais, c'est l'individu qui est sacralisé et le droit administratif devient un outil de protection des droits individuels contre l'administration »[2182]. Cela ne signifie pas que le droit administratif doit satisfaire aveuglément les exigences du citoyen au détriment de l'intérêt général, ce qui nous ferait « vivoter dans une démocratie de la revendication et du ressentiment »[2183], une démocratie fondée sur la méfiance de chacun. Bien plus subtilement, il revient au droit administratif d'assurer le délicat équilibre entre la protection de droits individuels et l'intérêt général. Dans l'e-gouvernement, cet exercice se traduit par la recherche de solutions qui créent un équilibre entre le souci de protéger la vie privée des individus et d'encourager l'efficacité administrative.

En étant attentif à protéger le citoyen, le droit administratif éradique le risque, dénoncé dans notre recherche, que l'e-gouvernement crée un déséquilibre inadmissible entre le citoyen, transparent pour l'administration, et l'administration, opaque aux yeux du citoyen. Mais, plus encore, le droit administratif ainsi envisagé rééquilibre la relation entre l'administration et le citoyen. Il organise une relation plus égalitaire qu'elle ne l'était dans l'administration traditionnelle agissant en dehors des considérations de protection de la vie privée des citoyens. Il peut ainsi être soutenu que « si le privilège de l'unilatéralité paraît impossible à éradiquer dans la mesure où il relève de l'essence même du phénomène administratif, en revanche, le renforcement des garanties juridiques accordées aux administrés, tant en aval qu'en amont de l'action administrative, peut permettre de le contrebalancer, en contribuant par là à un rééquilibrage en profondeur du droit administratif »[2184].

(dir. H. DUMONT, P. JADOUL, B. LOMBAERT, F. TULKENS, S. VAN DROOGHENBROECK), t. 1, Bruxelles, La Charte, 2009, p. 483.

[2182] P. MARTENS, « Que reste-t-il du droit administratif ? », *A.P.T.,* 2006, p. 2. Dans le même sens, J. CHEVALLIER, « Les fondements du droit administratif à l'épreuve de l'Europe », *op. cit.,* p. 49.

[2183] P. MARTENS, *op. cit.,* p. 6.

[2184] J. CHEVALLIER, « Le droit administratif, un droit de privilège ? », *op. cit.,* p. 70.

Ainsi donc, alors que notre recherche a débuté en constatant que l'e-gouvernement menace d'aggraver dangereusement le déséquilibre existant entre l'administration et le citoyen, elle se conclut en affirmant que l'e-gouvernement peut aussi être une chance de rééquilibrer cette relation, pour autant que le droit administratif s'adapte aux enjeux de l'e-gouvernement et aux exigences du régime juridique de la protection de la vie privée et des données à caractère personnel. Cette adaptation du droit administratif est nécessaire, sous peine de « compromettre sa légitimité et sa survie »[2185]. Pour ce faire, le droit administratif doit tenir compte de plusieurs évolutions qui, chacune, révèlent une prise en compte plus importante du citoyen dans l'organisation et le fonctionnement de l'administration.

1. La protection du citoyen par le législateur. L'e-gouvernement modifie le rôle du législateur par rapport à l'administration. Un double mouvement s'engage. Le droit exige du législateur qu'il encadre l'administration de manière plus serrée. Dans le même temps, le législateur doit aussi renoncer à certaines interventions compte tenu de la rapidité et de la complexité de la technique, qu'il parvient difficilement à encadrer précisément.

Le droit à la protection de la vie privée et des données à caractère personnel est consacré par l'article 22 de la Constitution et par des normes supranationales. Il est interprété par les juges, spécialement par la Cour constitutionnelle et la Cour européenne des droits de l'homme. Ce droit exige du législateur qu'il définisse lui-même les éléments essentiels des traitements de données à caractère personnel effectués dans l'administration. La protection du citoyen apparaît en filigrane de cette solution. Comme l'ont affirmé la Cour constitutionnelle et la Cour européenne des droits de l'homme, si l'intervention du législateur est exigée, c'est pour garantir que les éléments essentiels des traitements de données fassent l'objet d'un débat entre les parlementaires que le citoyen a élus, et que ces éléments figurent dans une norme accessible et prévisible pour chacun. De cette manière, les traitements de données sont plus visibles et mieux compris par les citoyens. Ils sont également plus aisément contestables.

La définition des éléments essentiels des traitements de données par le législateur conduit à nuancer certains enseignements traditionnels du droit administratif. On ne peut plus affirmer que la compétence d'organiser l'administration ressortit à la compétence exclusive du Roi. Dans l'e-gouvernement, il revient au législateur, et non au Roi, d'organiser

[2185] J. CHEVALLIER, « Les fondements du droit administratif à l'épreuve de l'Europe », *op. cit.,* p. 50.

l'administration dans les aspects qui constituent des éléments essentiels des traitements de données. Ainsi, en regroupant des administrations au sein d'un réseau sectoriel, par exemple, le législateur intervient directement dans l'organisation de l'administration. Par ailleurs, on ne peut plus affirmer sans nuance que les administrations peuvent choisir, de manière discrétionnaire, les moyens qu'elles utilisent. Par exemple, les infinies possibilités de stockage, de transmission et de croisement de données informatisées créent des risques pour la protection de la vie privée des citoyens qui n'existaient pas avec l'utilisation de fiches en papier. C'est pourquoi, les administrations ne peuvent notamment plus décider elles-mêmes des informations qu'elles enregistrent dans leur base de données, ni les communiquer librement à d'autres administrations.

Néanmoins, bien que le droit fondamental à la protection de la vie privée et des données à caractère personnel exige du législateur qu'il intervienne davantage dans l'organisation de l'administration, il faut aussi reconnaître que le législateur est dépassé par la rapidité et la technicité des traitements de données à caractère personnel. Il doit définir les éléments essentiels mais ne pourrait en déterminer chaque détail. L'action du législateur dans l'e-gouvernement doit donc être soutenue par des relais qui contrôlent les traitements de données sur le terrain. Les détachés à la protection des données peuvent assurer ce rôle au sein des administrations. En outre, la Commission de la protection de la vie privée joue un rôle essentiel dans la régulation des traitements de données à caractère personnel.

2. La protection du citoyen par l'autorité indépendante de protection des données. L'administration agit aujourd'hui sous le contrôle de la Commission de la protection de la vie privée. Cette autorité indépendante incarne à elle seule plusieurs évolutions du droit administratif.

L'existence de la Commission de la protection de la vie privée confirme l'idée selon laquelle la *protection du citoyen doit être renforcée dans l'e-gouvernement*. Il ne s'agit plus seulement de donner au citoyen les moyens d'agir en justice pour sanctionner les illégalités commises par l'administration. Il existe désormais une autorité qui s'en charge elle-même, au nom des individus. Elle agit comme un « bouclier qui protège efficacement les citoyens contre les dangers de l'informatique »[2186]. À cet égard, l'action d'intérêt collectif que peut intenter la Commission de la protection de la vie privée est particulièrement intéressante car les citoyens n'exercent pas les voies d'action qui sont leur sont offertes à

[2186] J.-L. Missika et J.-P. Faivret, « Informatique et libertés », *Les Temps modernes*, 1977, n° 375, p. 322.

titre individuel pour sanctionner les utilisations abusives de leurs données personnelles dans l'e-gouvernement. Cela s'explique sans doute par le coût financier d'une action judiciaire, mais également par le fait que, bien souvent, les citoyens ignorent l'existence d'abus dans l'utilisation de leurs données.

Par ailleurs, les questions qui entourent le statut de la Commission de la protection de la vie privée rappellent la *colonisation du droit administratif par le droit européen*[2187]. La directive 95/46 et, prochainement, le règlement européen sur la protection des données à caractère personnel imposent l'indépendance de l'autorité de protection des données. Dans deux arrêts récents, la Cour de justice de l'Union européenne a donné une portée particulièrement large à cette exigence d'indépendance. Une fois réceptionnée par le droit belge, on s'aperçoit que cette interprétation est difficile à combiner avec certains principes constitutionnels et la jurisprudence de la Cour constitutionnelle à ce sujet. En effet, pour satisfaire au droit européen, la Commission de la protection de la vie privée ne peut pas être soumise au contrôle d'un ministre tandis que la Cour constitutionnelle exige qu'un ministre puisse être interpellé par le Parlement du fait des agissements de l'autorité indépendante, exigence qui est difficilement tenable si le ministre ne peut pas contrôler ladite autorité du fait même de l'indépendance de cette dernière… Face à la tension entre l'indépendance et la responsabilité de l'autorité de protection des données, une solution pourrait être de consacrer, dans la loi, la notion d'autorité administrative indépendante et d'en définir le statut. Une autre solution pourrait être d'organiser le contrôle direct du Parlement sur l'autorité indépendante, sans passer par l'intermédiaire d'un ministre.

Enfin, l'action de la Commission de la protection de la vie privée conduit à un *assouplissement du droit administratif*. Cette autorité de régulation tente de concilier les intérêts conflictuels que sont la protection de la vie privée des citoyens et l'efficacité de l'administration. Pour ce faire, elle dispose de plusieurs moyens. Certains s'apparentent aux moyens juridiques classiques, tels que le pouvoir d'agir en justice ou celui de dénoncer les infractions au procureur du Roi. Elle en use peu. Elle préfère se tourner vers les moyens d'action plus souples, avec lesquels elle essaie de convaincre plutôt que de contraindre[2188]. La Commission de la protection de la vie privée privilégie ainsi la médiation et l'émission d'avis et de recommandations. On doit y voir « un exemple de l'abandon

[2187] P. Martens *op. cit.,* p. 4 ; J.-B. Auby, *op. cit.,* p. 926 ; J. Chevallier, « Les fondements du droit administratif à l'épreuve de l'Europe », *op. cit.*, p. 37.

[2188] P. Martens, *op. cit.,* p. 5.

par le législateur des modes traditionnels de règlement des conflits »[2189]. Bien que cette manière d'agir soit utile, elle manque d'efficacité dans l'e-gouvernement. C'est pourquoi, il serait judicieux d'octroyer de nouveaux moyens d'action à la Commission de la protection de la vie privée qui, tout en tenant compte de la réticence de cette autorité à saisir les cours et tribunaux, soient plus contraignants que les solutions actuellement appliquées. On pense à l'octroi de pouvoirs d'injonction, d'admonestation et d'amende qui permettraient à la Commission de la protection de la vie privée d'obtenir rapidement de l'administration qu'elle mette fin aux traitements illégaux en cours d'exécution.

3. La protection du citoyen par la technologie. De nouveaux principes guident l'organisation de l'administration. Ils sont empreints du souci de protéger le citoyen contre l'usage abusif de ses données personnelles par l'administration mais aussi de faciliter ses relations avec l'administration. Ils consistent à utiliser la technologie non pas au détriment de la vie privée des citoyens, mais bien pour protéger ce droit fondamental. En d'autres termes, la technologie peut, certes, être un problème. Mais ces principes montrent qu'elle peut aussi être une solution.

Ainsi, l'importance du principe de « Privacy by design » a été soulignée. Dès la mise en place d'un outil de traitement, il convient de veiller à assurer la protection de la vie privée des individus dont les données seront traitées, lors de la configuration des outils, de la mise en place de logiciels, etc. De cette manière, la protection du citoyen est techniquement assurée par l'outil lui-même avant même d'être organisée par des normes juridiques. Cela conduit, par exemple, à encourager la décentralisation des données en les disséminant au sein de plusieurs sources authentiques de données dont l'accès est techniquement contrôlé plutôt que de les regrouper au sein d'une seule grande base de données.

Les développements relatifs à la transparence de l'e-gouvernement ont montré l'importance du *principe de la réciprocité des avantages*. S'inscrivant dans le prolongement de la loi du changement, ce principe impose à l'administration de conférer au citoyen certains avantages liés à la technologie, en compensation de ceux dont elle bénéficie pour accomplir ses propres missions. Appliqué à la transparence de l'administration, ce principe permet au citoyen d'exiger notamment de pouvoir consulter, depuis son ordinateur, ses données au sein de l'administration et d'identifier les institutions qui ont utilisé ces données.

[2189] F. RIGAUX, « Chapitre 3. Les paradoxes de la protection de la vie privée », *op. cit.*, p. 39.

En définitive, l'e-gouvernement donne au droit administratif une troisième dimension. La première dimension du droit administratif est celle qu'il a toujours eue. Elle consiste à encadrer l'organisation et le fonctionnement de l'administration. La deuxième dimension du droit administratif est apparue dans les années nonante avec le mouvement d'ouverture vers le citoyen qui s'est engagé à la faveur des règles de transparence administrative. La troisième dimension du droit administratif naît dans le contexte de l'e-gouvermenent. Désormais, le droit administratif doit être un outil de protection du citoyen contre l'administration qui abuserait de ses données à caractère personnel.

Ainsi donc, au-delà de son apparente technicité, l'e-gouvernement apparaît aujourd'hui comme une chance offerte au droit administratif de rapprocher l'administration du citoyen, en se nourrissant de l'idéal humain fort qui désormais l'irrigue, celui de protéger la vie privée des individus et de contribuer ainsi à assurer les conditions de leur libre épanouissement personnel.

* * *

Bibliographie

La présente bibliographie est sélective. Elle ne reprend que les sources doctrinales les plus utilisées dans le cadre de notre recherche doctorale.

I. Monographies

ANDERSEN R., DÉOM D. ET RENDERS D. (dir.), *Les sanctions administratives*, Bruxelles, Bruylant, 2007.

BATSELE D., MORTIER T. et SCARCEZ M., *Manuel de droit administratif,* Bruxelles, Bruylant, 2010.

BOES M. et SUETENS L.-P., *Administratief recht,* Leuven, Acco, 1994.

BOUVIER P., *Éléments de droit administratif,* Bruxelles, De Boeck, 2002.

CAMBIER C., *Droit administratif*, Bruxelles, Larcier, 1968.

COLLARD C.-A. ET TIMSIT G., *Les autorités administratives indépendantes,* Paris, PUF, 1988.

CORNELIS L., *Principes du droit belge de la responsabilité extra-contractuelle,* Bruxelles, Bruylant, Anvers, Maklu, 1991.

DE BOT D., *Verwerking van persoonsgegevens,* Anvers, Kluwer, 2001.

DE BOT D., *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank vanOndernemingen en de elecktronische identiteitskaart als belangrijkste juridische bouwstenen,* Brugge, Vandenbroele, 2005.

DELPÉRÉE F., *Le droit constitutionnel de la Belgique*, Bruxelles-Paris, Bruylant-L.G.D.J., 2000.

DE TERWANGNE C., *Société de l'information et mission publique d'information,* Namur, FUNDP, 2001, http://www.crid.be/pdf/public/These_cdeterwangne.pdf

DOCQUIR B. et PUTTEMANS A., *Actualités du droit de la vie privée,* Bruxelles, Bruylant 2008.

DOYEN-BIVER C., DURVIAUX A.-L., FISSSE D., et SOHIER J., *La responsabilité des pouvoirs publics,* Kluwer, Waterloo, 2010,

DUASO CALES R., *Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau.Thèsede doctorat présentée à la faculté de droit de l'Université de Montréal et à la faculté de droit de l'Université de Paris II,* septembre 2011.

DUMONT H., JADOUL P., LOMBAERT B., TULKENS F. et VAN DROOGHENBROECK S., *Le service public, 1. Le service public : passé, présent et avenir,* Bruxelles, La Charte, 2009.

DUMONT H., JADOUL P., LOMBAERT B., TULKENS F. et VAN DROOGHENBROECK S., *Le service public, 2. Les « lois » du service public,* Bruxelles, La Charte, 2009.

ERGEC R., *Les droits économiques, sociaux et culturels dans la Constitution. Actes du colloque tenu à l'Université Libre de Bruxelles les 21 et 22 décembre 1994,* Bruxelles, Bruylant, 1995.

ERGEC R., *Introduction au droit public,* Tome II, Bruxelles, Kluwer, 2003.

ERGEC R., *Protection européenne et internationale des droits de l'homme,* Bruxelles, Bruylant, 2004.

GOFFAUX P., *Dictionnaire élémentaire de droit administratif*, Bruxelles, Bruylant, 2006.

GRAUX H. et DUMORTIER J., *Privacywetgeving in de praktijk,* Courtai, UGA, 2009.

HABERMAS J., *L'espace public*, Paris, éd. Payot, 1997.

HERBIET M. et DURVIAUX A.-L., *Droit public économique,* Bruxelles, La Charte, 2008.

JONGEN F., *La police de l'audiovisuel. Analyse comparée de la régulation de la radio et de la télévision en Europe,* Bruxelles, bruylant, L.G.D.J., Paris, 1994.

KOMMERS D.P., *The Constitutional Jurisprudence of the Federal Republic of Germany*, 2nd ed., Durham and London, Duke University Press, 1997, pp. 322 à 327.

LEROY M., *Contentieux administratif,* 5e éd., Limal, Anthemis, 2011.

LEWALLE P., *Contentieux administratif,* 3e éd., Bruxelles, Larcier, 2008.

MARGUÉNAUD J.-P., *La Cour européenne des droits de l'homme,* 4e éd., Paris, Dalloz, 2008.

MAST A., DUJARDIN J., VAN DAMME M. et VANDE LANOTTE J., *Overzicht van het Belgisch Administratief Recht,* 18e éd., Malines, Kluwer, 2009.

MATHIEU, B., *La loi,* Paris, Dalloz, 1996.

MESSADIÉ G., *La fin de la vie privée,* Paris, Calmann-Lévy, 1974.

NIHOUL M., *Les privilèges du préalable et de l'exécution d'office,* Brugge, La Charte, 2001.

OPDEBEEK I. et COOLSAET A., *Formele motivering van bestuurshandelingen,* Brugge, die Keure, 1999.

PATRICK A.S. et KENNY S., *From Privacy Legislation to Interface Design : Implementing Information Privacy in Human-Computer Intercations*, Springer-Verlag Berlin Heildelberg, 2003, pp. 107-124.

QUERTAINMONT P., *Droit public économique. Interventionisme économique et avenir,* Waterloo, Kluwer, 2007.

RENDERS D., BOMBOIS T., GORS B., THIEBAUT C. et VANSNICK L., *Droit administratif. Tome III. Le contrôle de l'administration,* Bruxelles, Larcier, 2010.

RIGAUX F., *La protection de la vie privée et des autres biens de la personnalité,* Bruxelles-Paris, Bruylant-L.G.D.J., 1990.

ROUX A., *La protection de la vie privée dans les rapports entre l'État et les particuliers,* Pris, Economia, 1983.

STASSINOPOULOS M., *Le droit de la défense devant les autorités administratives,* Paris, L.G.D.J., 1976.

SALMON J., *Le Conseil d'État de Belgique,* Bruxelles, Bruylant, 2012.

UYTTENDAELE M., *Précis de droit constitutionnel belge*, Bruxelles, Bruylant, 2005.

VANDE LANOTTE J. et GOEDERTIER G., *Handboek Belgisch Publiekrecht*, Brugge, die Keure, 2010.

VANDENBERGHE H., VAN OEVELEN A., VUYE H., WYNANT L. et VANDENBERGHE H. (dir.) *Overheidsaansprakelijkhei*d, Brugge, die Keure, 2005.

VAN DEN HOVEN VAN GENDEREN R. et VAN SCHELVEN P., *E-government : virtuele fictie of blijvend toekomstbeeld ?,* Elsevier, 2001, 92 p.

VAN SPEYBOROECK J.P., *De gemeentelijke registers en de privacybescherming. Eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonesgegevens in de bevolkingsregisters en in andere bestanden,* Brugge, die Keure, 1995.

VAN DER VORST P., *Le paysage informatique de la sécurité sociale comme métaphore ?,* 3e éd., Bruxelles, Bruylant, 2011.

VAUTROT-SCHWARZ C., *La qualification juridique en droit administratif,* Paris, L.G.D.J., 2009.

VERDUSSEN M., *Justice constitutionnelle,* Bruxelles, Larcier, 2012.

VITALIS A., *Informatique, Pouvoir et Libetés,* Paris, Economica, 2e éd., 1988.

WAETERINCKX P., *De strafrechtelijke verantwoordelijkheid van de rechtspersoon en zijn leidinggevenden. Een analyse vanuit de rechts- en bedrijfspraktijk*, Anvers, Intersentia, 2011.

WILKIN R., *L'administration publique belge*, Bruxelles, Bruylant, 1958.

X., *Openbaarheid van bestuur in Vlaanderen, België en de Europese Instellingen,* Instituut voor Administratief Recht van de KULeuven, Leuven, 1996.

II. Ouvrages collectifs et contributions

ALLEN A. A., « Constitutional law and privacy », *in A Comanion to Philosophy of Law and Lega Theory* (dir. D. PATTERSON), Cambridge/oxford, Blackwell Publishers, 1996, pp. 139-155.

ALLAND D. et RIALS S. (dir.), *Dictionnaire de la culture juridique*, Paris, P.U.F., 2003.

ANDRIANTSIMBAZOVINA J., « L'État et la société démocratique dans la jurisprudence de la Cour européenne des droits de l'homme », *in X. Libertés, justice, tolérance. Mélanges en l'hommage au Doyen Gérard Cohen-Jonathan,* Bruxelles, Bruylant, 2004, vol. I, pp. 59 et s.

BARNES J., « The meaning of the principle of proportionnality for the administration », in (dir. H. BAUER et C. CALLIES). *Verfassungsprinzipien in Europa, Constitutional principles in Europa, Principes constitutionnels en Europe*, Athènes, Berlin, Bruxelles, Ant. N. Sakkoulas, Berliner wissenschaft-verlag, Bruylant, 2008, pp. 219-247.

BENOIT ROHMER F., « Valeurs et droits fondamentaux dans le Traité de Lisbonne », *in Le Traité de Lisbonne. Reconfiguration ou déconstitutionnalisation de l'Union europeénne ?* (dir. E. BROSSET, C. CHEVALLIER-GOVERS, V. EDJAHARIAN et C. SCHNEIDER), Bruxelles, Bruylant, 2009, pp. 143-164.

BENYEKHLEF K. et TRUDEL P. (dir.), *État de droit et virtualité*, Montréal, Éd. Thémis, 2009.

BRAIBANT G., « Droit d'accès et droit à l'information », *in Services public et libertés. Mélanges offerts au professeur Robert-Edouard Charlier*, Paris, Éd. de l'Université et de l'enseignement moderne, 1981, pp. 703 et s.

BUNDSHUCH-RIESENEDER, F., « Governance and e-governance in the frame of Bologna process », *in Bologna Process, European construction European Neighbourhood Policy* (dir. T. COME et G. ROUET), Bruxelles, Bruylant, 2011, pp. 253 à 262.

CHATILLON G. et DU MARAIS B., *L'Administration électronique au service des citoyens,* Bruxelles, Bruylant, 2003.

CHATILLON G. (dir.), *Droit de l'administration électronique. De nouveaux droits pour les usagers. Des nouvelles règles pour les agents,* Bruxelles, Bruylant, 2011.

CHEVALLIER J., « Les fondements idéologiques du droit administratif français », *in Variations autour de l'idéologie de l'intérêt général*, Paris, Puf, 1979, pp. 3-57.

CHEVALLIER J., DRAÏ R. et RANGEON F. (dir.), *La communication administration – administrés*, Paris, PUF, 1983.

CHEVALLIER J., « Le mythe de la transparence adminisrative », *in Information et transparence administratives* (dir. F. RANGEON et al.), Paris, Puf, 1988, pp. 239-275.

CLAES E., DUFF A. et GURTWIRTH S. (dir), *Privacy and the criminal law*, Antwerpen-Oxford, Intersentia, 2006.

DEGRAVE E. et POULLET Y., « Le droit au respect de la vie privée face aux nouvelles technologies », in *Les droits constitutionnels en Belgique* (dir. M. VERDUSSEN et N. BONBLED), Bruxelles, Bruylant, 2011, pp. 1001-1035.

DELGRANGE X., DETROUX L. et DUMONT H., « La régulation en droit public » *in Elaborer la loi aujourd'hui, mission impossible ?,* (dir. B. JADOT et F. OST), Bruxelles, Publications des Facultés universitaires Saint-Louis, 1999, pp. 35-106.

DEMEZ G., « La preuve en droit du travail : protection de la vie privée et nouvelles technologies. Du contremaître à la cybersurveillance », *in X, Questions de droit social,* Liège, Formation permanente CUP, 2002, pp. 289-334.

DÉOM D., « Les instruments du droit administratif à l'épreuve des 'partenariats public-privé' (P.P.P.)», *in Les partenariats public-privé (P.P.P.) : un défi pour le droit des services public* (dir. B. LOMBAERT), Bruxelles, La Charte, 2005, pp. 190 à 230.

DE ROY D., « Le pouvoir réglementaire des autorités administratives indépendantes en droit belge », in *Rapports belges au Congrès de l'Académie internationale de droit comparé à Utrecht,* Bruxelles, Bruylant, 2006, pp. 711-747.

DE ROY D., « La nature des prétentions de l'usager au bénéfice des prestations de service public : essai de typologie », in *Le service public : passé, présent et avenir* (dir. H. DUMONT, P. JADOUL, B. LOMBAERT, F. TULKENS, et S. VAN DROOGHENBROECK), T. 1, Bruxelles, La Charte, 2009, pp. 483-527.

DE SCHUTTER O., « Article II-68 », in *Traité établissant une Constitution pour l'Europe. Comentaire article par article. Partie II. La Charte des droits fondamentaux de l'Union* (dir. L. BURGOGUE-LARSEN, A. LEVADE et F. PICOD), Bruxelles, Bruylant, 2005, pp. 122-152.

DE TERWANGNE C., « Le Rapport de la vie privée à l'information », *in Droit des technologies de l'information. Regards prospectifs à l'occasion des vingt ans du CRID* (dir. E. MONTERO), Bruxelles, Bruylant, 1999, pp. 137-149.

DE TERWANGNE C., « Protection des données à caractère personnel : application en Belgique de la directive européenne », *in Actualités du droit des technologies de l'information et de la communication,* Formation Permanente CUP, 2001, pp. 5-34.

DE TERWANGNE C., « Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles : regards croisés sur deux voies d'accès à l'information », *in Transparence et droit à l'information*, Liège, Formation Permanente CUP, 2003, pp. 85 à 115.

DE TERWANGNE C., « Introduction – La protection des données à caractère personnel et l'e-gouvernement » *in Défis du droit à la protection de la vie privée,* Bruxelles, Bruylant, 2009, pp. 505-511.

DOCQUIR B., « Le droit de la vie privée : aperçu général et règle de proportionnalité », *Actualités du droit de la vie privée* (dir. B. DOCQUIR et A. PUTTEMANS) Bruxelles, Bruylant, 2008, pp. 1-38.

DOMMERING E. et ASSCHER L. (dir.), *Coding regulation. Essays on the Normative Role of Information technology,* La Haye, TMC Asser Press, 2006.

DOURMONT O. et BATSELÉ D., « 1985-1989 : cinq années de jurisprudence du Conseil d'État relative aux principes généraux du droit administratif », *A.P.T.,* 1990, pp. 262-308.

DUMONT H., JADOUL P., LOMBAERT B., TULKENS F. et VAN DROOGHENBROECK S. (dir.), *Le service public. 2. Les 'lois' du service public* », Bruxelles, La Charte, 2009.

DUMORTIER J. et ROBBEN F. (dir.), *Persoonsgegevens en privacybescherming* Brugge, die Keure, 1995.

FAVREAU B., « La protection des données à caractère personnel », *in La Charte des droits fondamentaux de l'Union européenne après le Traité de Lisbonne* (dir. B. FAVREAU), Bruxelles, Bruylant, 2010, pp. 185 et s.

GUADAMUZ A., « Habeas Data vs the European Data protection Directive », *The Journal of Information, Law and Technology,* 2001 (3), disponible sur Available at SSRN : http://ssrn.com/abstract=569106 (18 pages)

HAUSMANN J.-M., « Le droit d'accès au système d'information santé organisé par le décret du 16 juin 2006 de la Communauté flamande », *in Évolution des droits du patient, indemnisation sans faute des dommages liés aux soins de santé : le droit médical en mouvement* (dir. G. SCHAMPS), Bruxelles, Bruylant, Paris, L.G.D.J., 2007, pp. 187-247.

HAVELANGE B. et POULLET Y., « Secret d'État et vie privée : ou comment concilier l'inconciliable ? » *in Droit des technologies de l'information : regards prospectifs* (dir. E. MONTERO), Bruxelles, Bruylant, 1999, pp. 223-257.

HERVEG J., « La procédure 'comme en référé' appliquée aux traitements de données », *in Les actions en cessation,* Bruxelles, Larcier, 2006, pp. 215-246.

HEUSCHLING L., « État de droit, Étude de linguistique, de théorie et de dogmatique juridiques comparées » i*n X. Verfassungsprinzipien in Europa, Constitutional principles in Europa, Principes constitutionnels en Europe* (dir. H. BAUER et C. CALLIES), Athènes, Berlin, Bruxelles, Ant. N. Sakkoulas, Berliner wissenschaft-verlag, Bruylant, 2008, pp. 103-155.

HUBERLANT Ch., « Le droit de défense devant l'autorité d'administration active », *A.P.T.*, 1978-79, pp. 1-16.

HONDIUS F.W., « Een grondrecht op databescherming ? », *Jurist en Computer* (dir. A.H. DE WILD et B. EILDERS), Kluwer, Deventer, 1983, pp. 171-181.

JAUMOTTE J., « Les principes généraux du droit administratif à travers la jurisprudence administrative », *in Le Conseil d'État de Belgique, Cinquante ans après sa création (1946-1996),* (B. BLERO éd.), Bruxelles, Bruylant, 1999, pp. 593-696.

JOASSART P., « De la nature administrative des décisions de l'ONSS et de ses conséquences », *in La sécurité sociale des travailleurs salariés. Assujettissement, cotisations et sanctions* (dir. J.-F. NEVEN et S. GILSON), Bruxelles, Larcier, 2010, pp. 481-503.

JONES R.V., « La vie privée mise en péril par la technologie », *in Vie privée et drtois de l'homme. Actes du 3e colloque sur la Convention européenne des droits de l'homme (Bruxelles, 30 septembre – 30 octobre 1970),* Bruxelles, Bruylant, 1973, pp. 185-214.

JUVIGNY P., « Les réalisations scientifiques et techniques modernes et leurs conséquences sur la protection du droit au respect de la vie privée et familiale, du domicile et des communications », in *Vie privée et drtois de l'homme. Actes du 3e colloque sur la Convention européenne des droits de l'homme (Bruxelles, 30 septembre – 30 octobre 1970),* Bruxelles, Bruylant, 1973, pp. 171-183.

KIGANAHE D. et POULLET Y. (dir.), *Le secret professionnel,* Bruxelles, La Charte, 2002.

LÉONARD T., Observations sous Civ. Bruxelles (prés.), 22 mars 1994, *J.T.,* 1994, pp. 841-853.

MALARET E., « Droit, administrations publiques et NTIC : vers la restructuration de l'espace public. Les instruments pour la construction d'une démocratie dialogique », *in Études en l'honneur de Gérard Timsit,* Bruxelles, Bruylant, 2004, pp. 413-431.

MATHIEU B. et VERPEAUX M. (dir.), *L'intérêt général, norme constitutionnelle*, Paris, Dalloz, 2007.

MATHY I., « Etre ou ne pas être une personne juridique distincte de l'État, la Communauté ou la Région ? L'autonomie avec ou sans personnalité juridique », *in Le paraétatisme – Nouveaux regards sur la décentralisationfonctionnelle en Belgique et dans les institutions européennes* (dir. P. JADOUL, B. LOMBAERT et F. TULKENS), Bruxelles, la Charte, 2010, pp. 33 à 114.

MEGRET J., « De l'obligation de procéder à un examen particulier des circonstances de l'affaire », *Études et documents du Conseil d'État,* 1953, pp. 77-79.

MOENS, L., « Passieve openbaarheid van bestuur en privacybescherming », *in Het handvest van de sociaal verzekerde en bestuurlijke vernieuwing in de sociale zekerheid* (dir. J. PUT), Brugge, die Keure, 1999, pp. 208 à 275.

NEVEN J.-F., « Les principes généraux : les dispositions internationales et constitutionnelles », *in Vie privée du travailleur et prérogatives patronales* (dir. J.F. LECLERCQ *et alii*), Bruxelles, Éd. du Jeune Barreau, 2005, pp. 15-53.

NEVEN J.-F. et DE ROY D., « Principes de bonne administration et responsabilité de l'ONSS », *in La sécurité sociale des travailleurs salariés. Assujettissement, cotisations et sanctions* (dir. J.-F. NEVEN et S. GILSON), Bruxelles, Larcier, 2010, pp. 507-564.

NIHOUL M. (dir.), *La responsabilité pénale des personnes morales en* Belgique, Bruxelles, La Charte, 2005.

NIHOUL M. (dir.), *L'article 159 de la Constitution. Le contrôle de légalité incident*, Bruxelles, La Charte, 2010.

PÂQUES M., « Décentralisation, régulation et contrôle démocratique. L'arrêt 130/2010 en question », *Liber amicorum Marc Boes,* Brugge, die Keure, 2011, pp. 411 et s.

POULLET Y., « L'informatique menace-t-elle nos libertés ? », *in La télématique, T. 1 : Aspects juridiques, techniques et socio-politiques. Actes du colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit (CRID) des Facultés Notre-Dame de Namur,* Gand, Éd. Story-Scientia, 1984, pp. 191-208.

POULLET Y., DE TERWANGNE C. et TURNER P. (dir.), *Vie privée : nouveaux risques et enjeux – Privacy : new risks and opportunities,* Bruxelles, Éd. Story-Scientia, 1997.

POULLET Y., « Le droit et le devoir de l'union européenne et des États membres de veiller au respect de la protection des données dans le commerce mondial », *in Francisco Fernandez Segado (ed) Th Spanish Constitution in the European Constitutional context,* Madrid, Dykinson, 2003, pp. 1753 et s.

POULLET Y., « La protection des données : entre libertés, droits subjectifs et intérêts légitimes », *in Liber Amicorum Paul Martens,* Bruxelles, Larcier, 2007, 133-150.

POULLET Y., « Pour une troisième génération de réglementation de protection des données », *in Défis du droit à la protection de la vie privée,* coll. Cahiers du Centre de recherches Informatique et Droit, 31, Bruxelles, Bruylant, 2008, pp. 25-70.

PUTZEYS J., GEHLEN S. et BOURTEMBOURG J., « La bonne foi, critère d'appréciation dans l'acte administratif », *in La bonne foi (*dir. S. David-Constant), Éd. du Jeune Barreau de Liège, 1990, pp. 381-408.

QUÉNEUDEC J.P., « Liberté d'accès au droit et qualité des règles juridiques », *in Libertés, justice, tolérance. Mélanges en hommage au Doyen Gérard Cohen-Jonathan*, vol. II, Bruxelles, Bruylant 2004, pp. 1317-1326.

RANGEON F., LAVEISSIÈRE J. et BELIN P. (dir.), *Information et transparence administratives,* Paris, PUF, 1988.

RENDERS D. (dir.), *L'accès aux documents administratifs*, Bruxelles, Bruylant, 2008.

RENDERS D., BOMBOIS T., GORS B., THIEBAUT C. et VANSNICK L., *Droit administratif. Tome III. Le contrôle de l'administration,* Bruxelles, Larcier, 2010.

RINGELHEIM J., « Recueil de données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », *in Les nouvelles lois luttant contre la discrimination*, Brugge, La Charte, 2008, pp. 63-99.

RINGELHEIM J., « Recueil de données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », in *De nieuwe federale antidiscriminatiewetten-Les nouvelles lois luttant contre la discrimination*, die Keure, La Charte, Brugge, Bruxelles, 2008, pp. 63-100.

RIGAUX F. (dir.), *La vie privée : une liberté parmi les autres ?,* Bruxelles, Larcier, 1992.

PETTITI L.E., DECAUX E. et IMBERT P.-H. (dir.), *Convention européenne des droits de l'homme. Commentaire article par article*. Paris, Economica, 1999, 2e éd., pp. 305-321.

SAROT J. et DEROOVER W., « Le droit de la défense devant l'administration et le juge de celle-ci », *A.P.T.,* 1984, pp. 193-204.

SIMON D., « Le principe de 'bonne administration' ou la 'bonne gouvernance' concrète », in X, *Le droit de l'Union européenne en principes : liber amicorum en l'honneur de Jean Raux,* Rennes, Apogée, 2005, pp. 155-176.

SKOURIS V., « La protection des droits fondamentaux dans la jurisprudence de la Cour de justice : les étapes d'une consolidation progressive », *in La nouvelle Union européenne,* Bruxelles, Bruylant, 2006, pp. 87-112.

SUDRE F. « Les aléas de la notion de 'vie privée' dans la jurisprudence de la Cour européenne des drtois de l'homme », *in Mélanges en hommage à Louis Edmond Pettiti,* Bruxelles, Bruylant, 1998, pp. 704 et s.

SUETENS L.P. et LEYSEN R., « Staat, gewesten en gemeenschappen. De technieken van bevoegdheidsverdeling. De rol van het arbitragehof », *in X., Prof. Dr Louis Paul Baron Sueten, Op de grens van het ideaal denkbare en het praktisch haalbare,* Brugge, die Keure, 1997, pp. 223-250.

VANDE LANOTTE J. et HAECK Y. (dir.), *Handboek EVRM. Artikelsgewijze commentaar,* Anvers, Intersentia, 2004.

VAN DROOGHENBROECK S. et VELAERS J., « La répartition des compétences dans la lutte contre la discrimination », *in De nieuwe federale antidiscriminatiewetten-Les nouvelles lois luttant contre la discriminatin,* die Keure, La Charte, Brugge, Bruxelles, 2008, pp. 101-127.

VERDEYEN V., « Obligations des institutions de sécurité sociale », *La sécurité sociale en pratique* (dir. J. PUT, O. LANGLET et O. MORENO), Mechelen, Kluwer, 2009, pp. 5-12.

VERDEYEN V., « Informatisation de la gestion de la sécurité sociale », *La sécurité sociale en pratique* (dir. J. PUT, O. LANGLET et O. MORENO), Mechelen, Kluwer, 2009, pp. 13-25.

VEROUGSTRAETE I., « La procédure civile confrontée à l'ère de l'électronique », *Liber amicorum Paul Martens,* Bruxelles, Larcier, 2007, pp. 627-648.

X., *L'État de droit,* Paris, La documentation française, 2004.

III. Articles de revue, notes d'arrêt et observations

ANDERSEN R., « Observations. Les méfaits de la législation par référence », note sous Cass. (1re ch.), arrêt n° F 1126 F/1, du 10 octobre 1991, *Rev. dr. Comm.,* 1992, pp. 198-200.

ANDERSEN R., « Conclusions de la journée d'études sur les communes et la transparence administrative », *Rev. Dr. Comm.,* 1999, pp. 127-131.

ANDERSEN R., « La mise en balance des intérêts en cause dans l'appréciation des motifs d'exception à la publicité de l'administration », *C.D.P.K.,* 1999, pp. 38 et s.

ANDERSEN R. et LEWALLE P., « La motivation formelle des actes administratifs », *A.P.T.*, 1993, pp. 62-85.

ANDERSEN R. et NIHOUL P., « Le Conseil d'État – Chronique de jurisprudence 1994 (2e partie) », *R.B.D.C.*, 1995, p. 171-208

ANDERSEN R. et NIHOUL P., « Le Conseil d'État – Chronique de jurisprudence 1994 (1re partie) », *R.B.D.C*, 1995, p. 71-108

ANDERSEN R. et NIHOUL P., « Le Conseil d'État – Chronique de jurisprudence 1995 », *R.B.D.C*, 1996, p. 203-248

ANDERSEN R. et NIHOUL P., « Le Conseil d'État – Chronique de jurisprudence 1996 », *R.B.D.C*, 1997, p. 155-219

ANDERSEN R. et NIHOUL P., « Le Conseil d'État – Chronique de jurisprudence 1997 », *R.B.D.C*, 1998, p. 267-332

ANDERSEN R. et NIHOUL P., « Le Conseil d'État – Chronique de jurisprudence 1998 », *R.B.D.C*, 2000, p. 55-157

ANDERSEN R. et NIHOUL P., « Le Conseil d'État – Chronique de jurisprudence 1999 », *R.B.D.C*, 2000, p. 349-462

ANDERSEN R. et NIHOUL P., « Le Conseil d'État – Chronique de jurisprudence 2000 », *R.B.D.C*, 2002, p. 17-133

ANDERSEN R., NIHOUL P., et JOASSART M., « Le Conseil d'État – Chronique de jurisprudence 2001 », *R.B.D.C*, 2003, p. 125-238

ANDERSEN R., NIHOUL P., et JOASSART M., « Le Conseil d'État – Chronique de jurisprudence 2002 », *R.B.D.C*, 2004, p. 25-135

ARONSTEIN C.S., « Essai pour contribuer à la survie de notre civilisation », *J.T.,* 1971, pp. 453-460.

AULAGNON T. et JANICOT D., « Organisation méthodes et techniques. La communication entre Administration et Administrés », *Rev. Adm.,* 1975, pp. 311-319.

AUTEXIER C., « L'invention du droit fondamental 'à la garantie de la confidentialité et de l'intégrité des systèmes de la technologie de l'information'. Commentaire de la décision de la Cour constitutionnelle fédérale allemande du 27 février 2008 », *R.B.D.C.*, 2008/2, pp. 187-206.

BAEKELAND C., « De VZM als 'Administratieve overheid' in de zin van art. 14, §1, 1° RVS – Wet : De weg van de verwerkking tot de geboorte », *C.D.P.K.,* 2010, pp. 437-474.

BELEN V., « Les tentatives de protection des données personnelles des individus : difficultés de définition et risques nouveaux », *Market Management,* 2005/2, vol. 1, pp. 65-80.

BELORGEY J.-M., « L'État entre transparence et secret », *Pouvoirs,* 2001/2, n° 97, pp. 25-32.

BENEDEK C., « La transparence administrative en Belgique », *A.P.T.,* 1993, pp. 159 et s.

BODART J., « La protection de l'environnement par le biais du droit au respect de la vie privée et familiale et du domicile », *Amén.-Env.,* 2003, pp. 211 à 238.

BOULANGER M.-H., DE TERWANGNE C. et LÉONARD T., « La protection de la vie privée à l'égard des traitements de données à caractère personnel. La loi du 8 décembre 1992 », *J.T.,* 1993, pp. 369-388.

BOULANGER M.-H., CALLENS S. et S. BRILLON, « La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telel que modifiée par la loi [...] », *Rev. Dr. Santé,* 2000-2001, pp. 326-345.

BOSSUYT A., « Les principes généraux du droit dans la jurisprudence de la Cour de cassation », *J.T.*, 2005, pp. 725-736.

BRAIBANT G., « La protection des droits individuels au regard du développement de l'informatique », *Rev. Int. Dr. Comparé,* 1971, pp. 793-817.

BRAIBANT G., « Réflexions sur les perspectives d'évolution de l'administration », *R.F.A.P.*, 1979, pp. 179-199.

BRANS M., DE VISSCHER C. et VANCOPPENOLLE D., « Administrative Reform in Belgium : maintenance or modernisation », *West European Politics,* 2006, pp. 979-998.

BREMS E., « De nieuwe grondrechten in de Belgische Grondwet en hun verhouding tot het Internationale, inzonderheid het Europese Recht », *T.B.P.,* 1995, pp. 619-636.

BREMS E., « Grondwettelijke bescherming tegen geluidshinder », *T.V.M.*, 2003, pp. 385-389.

BRIBOSIA E. et DE SCHUTTER O., « La Charte des droits fondamentaux de l'Union européenne », *J.T.,* 2001, pp. 281-297.

BURKERT H., « Institutions of data protection – an attempt at a functional explanation of european national data protection laws », *Computer Law Journals*, 1981-82, pp. 167-188.

BURKERT H., « Le jugement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses conséquences », *D.I.T.,* 1985, n° 4, pp. 8-14.

BURKERT H., « La législation sur la protection des données et la modernisation des administrations publiques », *RISA*, 1996, pp. 669-682.

BURKERT H., « L'information du secteur public. Le secret, la transparence et le commerce », *Revue française d'administration publique,* 1994, pp. 581 et s.

BURKERT H., « Progrès technologique, protection de la vie privée et responsabilité politique », *Revue française d'Administration publique*, 1999, pp. 119-129.

BYGRAVE L., « Minding the machine : Article 15 of the EC Data Protection Directive and Automated Profiling », *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24.

CARBONE M., « Fichier central des avis de saisie, de délégation, de cession et de règlement », *J.T.,* 2011, pp. 781-787.

CARIAT N., « La Charte des droits fondamentaux de l'Union européenne et les juridictions belges. Quelques balises pour une application prometteuse », *J.T.,* 2010, pp. 105-110.

CHATILLON G., « L'Administration électronique : enjeux pratiques, défis juridiques », *Cahiers Lamy*, 2004, pp. 8-14.

CHEVALLIER J., « La régulation juridique en question », *Droit et société*, 2001/3, p. 827-846.

COENRAETS P., « Les accords de coopération dans la Belgique fédérale », *A.P.T.*, 1992, pp. 158 à 200.

DALCQ R., « Unité ou dualité des notions de faute et d'illégalité », *R.C.J.B.*, 1984, pp. 19-31.

DAMIEN R. et MATHIAS P., « Présentation », *Cités,* 2009/3, n° 39, pp. 9-12.

DE BISSCHOP K. et CARLIER E., « Klokkenluidersregelingen in een grensoverschrijdende context », *Or.,* 2009, pp. 48-60.

DE BOT D., « De Commissie voor de Bescherming van de Persoonlijke Levensfeer : Tussen droom en daad staan er niet alleen wetten in de weg, maar vooral praktische problemen », *R.G.D.C.-T.B.B.R.,* 2003, pp. 384-402.

DEGRAVE E., « La légalité pénale et la Cour d'arbitrage », *J.T.,* 2006, pp. 477-489.

DEGRAVE E., « La CPVP : un organisme invincible ? », *R.D.T.I.,* 2006, pp. 225 -241.

DEGRAVE E., « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée », *C.D.P.K.,* 2007, pp. 46-71.

DEGRAVE E. et POULLET Y., « L'Affaire Swift », *R.D.T.I.*, 2007, pp. 3-9.

DEGRAVE E., et POULLET Y., « L'externalisation de l'administration, les nouvelles technologies, et la protection de la vie privée », *J.T.,* 2008, pp. 277-285.

DEGRAVE E. et POULLET Y., « La création d'une institution en charge de la protection des données au sein de la Communauté française et/ou de la Région wallonne », *R.D.T.I.,* 2008, pp. 427-429.

DEGRAVE E., « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.,* 2009, pp. 365-371.

DEGRAVE E., « Arrêt 'Volker und Markus Schecke et Eifert' : le droit fondamental à la protection des données à caractère personnel et la transparence administrative », *J.D.E.,* 2011, pp. 97-99.

DEGRAVE E., « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données à caractère personnel illégal sanctionné par la Cour d'appel de Bruxelles », observations sous Bruxelles (9e ch.), 9 mai 2012, *J.T.,* 2012, pp. 691-693.

DE HERT P., « Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1991-1997 », *Jaarboek Mensenrechten 1996-1997,* pp. 43 et s.

DELGRANGE X., « La Cour d'arbitrage valide la loi du 29 juillet 1991. Qui peut consacrer le droit de l'administré à la motivation formelle des actes administratifs ? », *Journ. Jur.,* 2001, liv. 4, pp. 6-7.

DELPÉRÉE F. et BOUCQUEY-RÉMION V., « Liberté, légalité et proportionnalité », *A.P.T.,* 1979-1980, pp. 286-294.

DELPEREE F., « La Belgique est un État fédéral », *J.T.,* 1993, pp. 637-646.

DE MUL J., « Des machines morales », *Cités*, 2009/3, n° 39, pp. 27-38.

DE HERT P., « De grondrechten en wetten m.b.t. openbaarheid van bestuursdcument en bescherming van persoonlijke levensfeer. Analyse van de onderlinge relatie en commentaar bij het arrest Dewinter van de Raad van State », *C.D.P.K.,* 2001, pp. 390 et s.

DÉOM D., « Enseignement libre et autorité administrative : dis-moi oui, dis-moi non », note sous Cass., 25 septembre 2001, *A.P.T.,* 2004, pp. 95-106.

DE ROY D., « Regards croisés sur l'offre de services de la société de l'information par les communes », *R.D.T.I.,* 2002, pp. 53-77.

DE ROY D., « Etre ou ne pas être…autorité administrative. Vers de nouvelles questions existentielles pour les A.S.B.L. satellites des institutions communales ? », *Dr. Comm.,* 2002/2, pp. 200-216.

DE ROY D. et QUECK R., « De la téléphonie vocale aux offres publiques d'acquisition. Vers un 'droit de la régulation' ? », *J.T.,* 2003, pp. 553-563.

DE ROY D., « Le principe de continuité du service public et la situation de l'usager », note sous Cass, 12 février 2004, *R.C.J.B.,* 2005, pp. 201-247.

DE ROY D., « Les ressources de la jurisprudence de la Cour de cassation dans l'approche des missions de l'ONSS. Quelques réflexions », *J.T.T.,* 2005, pp. 435-429.

DE ROY D. et ROSIER K., « Publicité et transparence des marchés publics dématérialisés », *C.D.P.K.,* 2005, pp. 115-138.

De Roy D., *La gestion des moyens informatiques au service d'une administration électronique efficace. Quel rôle pour le Parlement de la Communauté française*, Bruxelles, Parlement de la Communauté française, 2006, disponible à l'adresse http://www.pfwb.be/le-travail-du-parlement/doc-et-pub/publications/gestionmoyensinformatiques.pdf (35 pages)

De Roy D., « Quelques aspects conceptuels et juridiques de la gestion de l'informatique publique », *in Services publics et mutualisation informatique : de la théorie à la pratique,* Bruxelles, Parlement de la Communauté française, 2006, pp. 7-14.

De Roy D., de Terwangne C. et Poullet Y., « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », *C.D.P.K.*, 2007, pp. 306 à 347.

De Roy D., « Le service public dans la tourmente », *J.T.,* 2007, p. 304.

De Roy D., « L'exception d'illégalité instituée par l'article 159 de la Constitution : de la vision d'apocalypse à la juste mesure ? », note sous Cass. 23 octobre 2006, *R.C.J.B.,* 2009, pp. 21-62.

De Roy D., « Stationnement payant, service public et partenariat public-privé », *J.T.,* 2009, pp. 574-575.

D. De Roy, « Établissements publics, organismes d'intérêt public et *tutti quanti* : la qualification juridique des satellites de l'administration », note sous Cass. 19 mars 2010, *R.C.J.B.,* 2013, pp. 34 à 97

De Salvia M., « Bilan de la jurisprudence de la Cour pour l'année 2001 », *R.U.D.H.*, 2002, pp. 126-168.

De Schutter O., « La vie privée entre droit de la personnalité et liberté », *R.T.D.H.,* 1999, pp. 827-863.

De Schutter O., « Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel », *R.T.D.H.,* 2001, pp. 148 et s.

De Schutter O., « Les droits fondamentaux dans l'Union européenne (1e janvier 2007-1er février 2008 », *J.D.E,* 2008, pp. 126-131.

De Schutter O., « Les droits fondamentaux dans l'Union européenne (1er février 2008-1er février 2009) », *JDE,* 2009, pp. 115-121.

De Schutter O., « Les droits fondamentaux dans l'Union européenne (1er janvier 2009-31 décembre 2009) », *J.D.E.,* 2010, pp. 120-127.

De Staercke J., « Le principe de bonne citoyenneté et le principe de chercher bon droit », *C.D.P.K.*, 2004, pp. 72-88 et pp. 211-225.

De Staercke J., « Algemene beginselen van behoorlijk burgerschap. Naar een wederkerig bestuurrecht ? », *Jura Falconis,* 2001-2002, pp. 505-535.

de Terwangne C., « Pour un cadre juridique d'une politique de diffusion des données détenues par le secteur public », *Cahiers Lamy du Droit de l'Informatique*, 1991, pp. 1-8.

de Terwangne C., « L'accès du public à l'information détenue par l'administration », *R.B.D.P.*, 1996, pp. 107-138.

de Terwangne C., « La Convention européenne des droits de l'homme et le droit de recevoir des informations de la part des autorités publiques », *Amén.,* 1998, pp. 265-270.

De Terwangne C. et Louveaux S., « La protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.,* 2001, p. 457-469.

de Terwangne C., « La nouvelle loi belge de protection des données à caractère personne », *Cahiers des sciences morales et politiques,* 2002, pp. 91-109.

de Terwangne C., « Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles », *Les petites affiches,* 2005, pp. 40-48.

de Terwangne C., « Vers une réévaluation de l'équilibre entre l'intérêt de la publicité des données et l'intérêt des personnes », *in Simplifiaction administrative et protection de la vie privée, un nouvel équilibre. Actes de la journée d'études du 15 octobre 2002,* Bruxelles, Agence pour la Simplification administrative, 2003, pp. 46-49.

De Terwangne C., « Réutilisation des informations du secteur public : la directive 2003/98 enfin totalement transposée en Belgique », *R.D.T.I.,* 2008, pp. 129 à 155.

de Terwangne C., « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 7 mai 2009*, College van burgemeester en wethouders van Rotterdam c. m.e.e. Rijkeboer*, aff. C-553/07, *R.D.T.I.,* 2011, pp. 79 et 80.

Dubuisson B., « Faute, illégalité et erreur d'interprétation en droit de la responsabilité civile », note sous Cass. (1e ch.), 26 juin 1998, *R.C.J.B.,* 2001, pp. 28-72.

Dumortier J. et Robben F., « Gebruikers-en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in Belgie », *Computerrecht,* 2009, pp. 37-60.

Durviaux A.-L., « La notion d'autorité administrative en débats », note sous C.E., n° 176.478 du 6 novrembre 2007, *C.D.P.K.,* 2008, pp. 854-858.

Ergec R., « La transparence administrative comme droit fondamental et ses limites », *A.P.T.,* 1993, pp. 87-95.

Ergec R., « L'Union économique et les marchés publics », *J.T.,* 1994, pp. 241-246.

Ergec R., « Le principe de légalité à l'épreuve des principes de bonne administration », *R.C.J.B.*, 1998, pp. 13-25.

Fabre-Alibert V., « La notion de 'société démocratique' dans la jurisprudence de la Cour européenne des droits de l'homme », *R.T.D.H.*, 1998, pp. 465-496.

Fagnart J., La responsabilité de l'administration du chef d'excès de pouvoir, *A.P.T.,* 1980, pp. 56-62.

Fauvet J., « La protection des données personnelles », *R.I.D.C.*, 1987, pp. 551-556.

Feld J., « Stationnement payant et traitements de données personnelles. Conjuguaison impossible ? », *R.D.T.I.,* 2008, pp. 485-500.

Frison-Roche M.-A., « Le droit de la régulation », *D.*, 2001, pp. 610-616.

Frison-Roche M.-A., « Définition du droit de la régulation économique », *D.* 2004, pp. 126-129.

Fromont M., « Le contrôle du respect du secret de la correspondance par une loi transposant une directive européenne », *R.T.D.H.*, 2010, pp. 937 et s.

Frydman B., « La transparence, un concept opaque ? », *J.T.*, 2007, p. 300.

GEELHAND N., « Le principe de la croyance légitime en droit administratif et en droit fiscal », *R.C.J.B.,* 1995, pp. 57-105.

GEUDENS G., « Arbitragehof schorst 'virtuele schanspaal' voor dopingzondaars », *Juristenkrant,* liv. 98, 2004, p. 13.

GLINEUR P., « La fiscalité et l'informatique… vers la naissance d'un droit fiscal de l'informatique », *R.G.F.,* 1984, pp. 75 et s.

GOFFAUX P., « Le régime juridique des recours administratifs inorganisés et organisés », *Rev. Dr. ULB,* 2008, pp. 201-228.

GREENLEAF G., « Promises and illusions of data protection in Indian Law », *International Data Privacy Law,* 2011, pp. 47 et s.

GREENLEAF G., « India's national ID system : Danger grows in a privacy vacuum », *Computer law and security review 2010,* pp. 479 à 491.

GREGORY J.D., « Solving Legal issues in Electronic Government : authority and authentification », C*anadian Journal of Law and technology*, 2002, pp. 1-19.

GUTWIRTH S., « De toepassing van het finaliteitsbeginsel van de privacywet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens », *T.P.R.,* 1993-II, pp. 1409-1468.

HAMEL M.-P., « Les transformations de l'État-providence néerlandais et l'accès aux droits sociaux », *Recherches et prévisions,* 2006, pp. 55 et s.

HAUBERT B. et VANDERNOOT P., « La nouvelle loi de réformes institutionnelles du 8 août 1980 », *A.P.T.,* 1988, pp. 211-267.

HUSTINX P., « COE and Data Protection : What has been Achieved ? », *Transnational Data and Communications Report,* Novembre 1989, pp. 21-22.

JANSSENS S., BOUDRY E., ROTTHIER S. et DE RYNCK F., « E-government : nieuwe kans of nieuw probleem ? Een onderzoek naar de ontwikkeling van ICT in Vlaamse gemeenten », *Bb&b,* 2010, pp. 211-230.

JUDO F., « Rechtsbescherming en federalisme : een nieuwe aflevering », *Juristenkrant*, 2001, liv. 30, p. 5.

KAISER V., « La Banque de données nationale générale et le droit d'accès indirect du citoyen aux données à caractère personnel qu'elle contient », *R.D.T.I.,* 2011, pp. 5-33.

KAUFF-GAZIN F., « Vers une conception européenne de l'indépendance des autorités de régulation », *Europe,* 2010, pp. 12-16.

KIRBY M., « The history, achievement and future of the 1980 OECD guidelines on privacy », International *Data Privacy Law,* 2011, pp. 6 et s.

KNAPP B., « La protection des données personnelles. Droit public suisse », *R.I.D.C.*, 1987, pp. 581-605.

KRANENBORG H.R., « Commentaar », *S.E.W.,* 2010, pp. 421-423.

KUMAYAMA K.D., « A right to pseudonymity », *Arizona Law Review*, 2009, vol. 51, pp. 427-464.

KUNER C., CATE F.-H., MILLARD C. et SVANTESSON D.J.B, « Editorial », *International Data Privacy Law,* 2011, p. 1.

LAGASSE D., « La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs », *J.T.*, 1991, pp. 737-738.

LAGASSE D., « Le principe de la séparation des pouvoirs en droti de la sécurité sociale », note sous Cass. 10 juin 1996, *R.C.J.B.* 1997, pp. 461-475.

LEJEUNE Y., « L'organisation des pouvoirs publics », *DIMM,* fasc. 53, Bruxelles, Story-Scientia, 2007, pp. 1 et s.

LÉONARD T. et POULLET Y., « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46.C.E. du 24 octobre 1995 », *J.T.,* 1999, pp. 377-396.

LOMBAERT B., « Discipline à l'armée, ordre illégal et vie privée », *R.T.D.H.,* 1996, pp. 303-313.

LOMBAERT B. et RIGODANZO V., « Quelques mises au point relatives au stationnement sur la voie publique », *R.R.D,* 2007, pp. 239-253.

LUST S., « Uitdrukkelijke motiveringswet doorstaat bevoegdheidscontrole », *Juristenkrant*, 2001, liv. 34, p. 7.

MAGREZ M., « La protection de la vie privée et la situation en allocations familiales pour travailleurs salariés », *Ann. Dr. Louv.,* 1984, pp. 121 à 126.

MAISL H., « État de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », *R.I.D.C.*, 1987, pp. 559-580.

MAISL H. et DU MARAIS B., « L'administration électronique », *Revue française d'administration publique,* 2004-2, pp. 211-216.

MALAURIE P., « L'intelligibilité des lois », *Pouvoirs,* 2005, n° 114, pp. 131-137.

MAN K., « De hoorplicht als algemmen beginsel van behoorlijk bestuur », *Jura Falconis,* 2005-2006, pp. 331-376.

MARCHETTI R., « L'arrêt du 19 janvier 2005 de la Cour d'arbitrage : une application du principe de proportionnalité dans le cadre de la législation sur la protection de la vie privée », *R.D.T.I.*, 2005, pp. 134-145.

MARTENS P., « Que reste-t-il du droit administratif ? », *A.P.T.*, 2008, pp. 1-6.

MASSET A., « La responsabilité pénale des personnes morales », *Droit pénal de l'entreprise,* 2011, pp. 3-16.

MATHIEU B., « Les lois de finance au crible de la sécurité juridique », *Les petites affiches*, 13 janvier 2006, pp. 4 et s.

MESSINE J., « Propos provisoires sur un texte curieux : la loi du 4 mai 1999 instituant la responsabilité pénale des personnes morale », *Rev. Dr. Pén.,* 2000, pp. 637-659.

MÉTALLINOS N., « La fonction de 'détaché à la protection des données' en Allemagne et aux Pays-Bas », *Droit social*, 2004, pp. 1066-1071.

MICHIELS O., « L'immunité pénale de certaines personnes morales de droit public et ses incidences sur le délai de prescpription de l'action civile née d'une infraction », *J.L.M.B.,* 2011, pp. 1542-1550.

MISSIKA J.-L. et FAIVRET J.-P., « Informatique et libertés », *Les temps modernes*, n° 375, pp. 314 et s.

MONETTE P.-Y., « Du contrôle de la légalité au contrôle de l'équité : une analyse du contrôle exercé par l'ombudsman parlementaire sur l'action de l'administration », *R.B.D.C.,* 2001, pp. 1-29.

MOUREAU L., « La signification du principe de légalité dans l'Administration moderne », *A.P.T.,* 1979-1980, pp. 282-285.

NIHOUL P., JOASSART M., et WILLEMART E., « Le Conseil d'État – Chronique de jurisprudence 2008 », *R.B.D.C.*, 2009, pp. 253-337.

NIHOUL P., JOASSART M. et FRANCK V., « Le Conseil d'État – Chronique de jurisprudence 2007 », *R.B.D.C.,* 2008, pp. 237-324.

NIHOUL P., JOASSART M. et FRANCK V., « Le Conseil d'État – Chronique de jurisprudence 2006 », *R.B.D.C.*, 2007, pp. 277-378.

NIHOUL P., JOASSART M. et FRANCK V., « Le Conseil d'État – Chronique de jurisprudence 2005 », *R.B.D.C.*, 2006, pp. 411-505.

NIHOUL P., JOASSART M. et FRANCK V., « Le Conseil d'État – Chronique de jurisprudence 2004 », Revue belge de droit constitutionnel, 2005, pp. 257-365

NIHOUL P. et JOASSART M., « Le Conseil d'État – Chronique de jurisprudence 2003 », R.*B.D.C.,* 2005, pp. 43-160

NIHOUL P., « La notion d'autorité administrative : retour à l'orthodoxie », *A.P.T., 2001*, pp. 78- 215.

NIHOUL M., « L'immunité pénale des collectivités publiques est-elle constitutionnellement correcte ? », *Rev. Dr. Pen.*, 2003, pp. 799-839.

NISSENBAUM H., « Protecting Privacy in a Information Age : the Problem of Privacy in Public », *Law and Philosophy,* 1998, vol. 17, pp. 559-596.

PAPAKONSTANTINOU V., « A data Protection Approach to Data Matching Operations Among Public Bodies », *International Journal of Law and Information Technology,* vol. 9, n° 1, pp. 39-64.

PÂQUES M., « L'application de la loi fiscale – Principes de bonne administration en droit administratif et en droit fiscal. Présentation et mise en œuvre », *Actualités du droit,* 1993, pp. 399-483.

PÂQUES M. ET DONNAY L., « Juridiction ordinaire et juridiction administratiev en droit belge », *Rapport présenté au colloque « La justice administrative dans les pays du Mahgreb- La réception des modèles européens », organisé les 2, 3, 4 novembre 2006 par l'association tunisienne de droit administratif et l'Unité de recherche en droit administratif de la Faculté de droit et des Sciences économiques et politiques de l'Université de Sousse*, disposnible sur http://orbi.ulg.ac.be/handle/2268/9929

POIDEVIN B., « La place des données personnelles dans l'administration électronique », *Expertises,* Janvier 2003, pp. 19-22.

PONTIER J.-M., « Qu'est ce que le droit administratif ? », *A.J.D.A.,* 2006, pp. 1937 à 1940.

POPELIER P., « De leer van beginselen van behoorlijk burgerschap blaast de figuur van rechtsverwerking nieuw leven in », note sous C.E. (12e ch.), 26 janvier 2006, n° 154.161, *R.W.*, 2006-2007, n° 2, pp. 57 à 59.

POULLET Y., « L'autorité de contrôle : 'vues' de Bruxelles », *Rev. Fr. Adm. Publ.,* 1999, pp. 69-81.

POULLET Y., « Internet et vie privée : entre risques et espoirs », *J.T.*, 2001, pp. 55 et s.

POULLET Y., « Quelques réflexions à propos de la délibération n° 19/2008 du 7 mai 2008 émanant du comité sectoriel registre national », *R.D.T.I.,* 2008, pp. 405-421.

POULLET Y. et DEGRAVE E., « La création d'une institution en charge de la protection des données au sein de la Communauté française et/ou de la Région wallonne », *R.D.T.I.,* 2008, pp. 427-429.

QUERTAINMONT Ph., « Le déclin de l'État de droit », *J.T.,* 1984, pp. 273-280.

RENSON A.-S., « L'indépendance des autorités de régulation : la fin d'un controverse », observasions sous C. Cst. 18 novembre 2010, *J.T.,* 2011, pp. 348-350.

RIBES D., « Existe-t-il un droit à la norme ? Contrôle de constitutionnalité et omission législative », *R.B.D.C.*, 1999, pp. 237 et s.

RIEDEL E.H., « Federal Constitutional Court Karlsruhe. Census Act 1983 partially unconstitutional », *Human Rights Law Journal,* 1984, pp. 94 à 116.

RIEDEL E.H., « New bearings in German data protection cenus act 1983 partially unconstitutional », *Human rights Journal,* 1984, pp. 67 à 93.

RIGAUX F., « Protection de la vie privée », *Ann. Dr. Louv.,* 1984, I, pp. 1 à 17.

RIGAUX F., « La liberté de la vie privée », *R.I.D.C.,* 1991, pp. 539-563.

RIGAUX F., « La protection de la vie privée à l'égard des données personnelles », *Ann. Dr. Louvain,* 1993, T. III, pp. 49-72.

RINGELHEIM F., « L'ordre informationnel », *Rev. b. dr. soc*, 1995, pp. 355-363.

RINGELHEIM F., « La protection des banques de données et la sécurité sociale », *Rev. Dr. ULB,* 1994-95, pp. 91-115.

ROUVROY A., « Pour une défense de l'érpouvante inopérabilité du droit face à l'opérabilité sans épreuve du comportementalisme numérique », *Dissensus, avril 2011, disponible sur http://popups.ulg.ac.be/dissensus/docannexe.php ?id=1269*

SCHARTUM D.W., « Designing and Formulating Data Protection Laws », *International Journal of Law and Technology,* 2008, vol. 18, pp. 1 et s.

SCHUTZ S., « Le délai raisonnable. Notion, origine, étendue, sanction et illustrations », *B.I.*, 2003/1, pp. 7-24.

SCHRAM F., « Openbaarheid van bestuur en de burgelijke stand », *T.B.P.*, 1998, pp. 391-397.

SCHRAM F., « Anderhalf jaar werking van de beroepinstantie Openbaarheid van bestuur », *C.D.P.K.*, 2006, pp. 545-546.

SCHRAM F., « Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer », *Bb&b.,* 2008, pp. 227 à 230.

SCORIELS V., « Le principe de confiance légitime en matière fiscale et la jurisprudence de la Cour de cassation », *J.T.,* 2003, pp. 301-310.

SILCOCK R., « What is e-government ? », *Parliamentary Affairs,* 2001, vol. 54, pp. 87 et s.

SNYDERS K. et SEGAERT S., « De onmiddellijke aangifte van tewerkstelling : een sleutelrol voor e-government in de sociale zekerheid », *T.S.R.,* 2003, pp. 74-106.

SNIJKERS K., « Management van interbestuurlijke e-government projecten », *Bb & b,* 2006, pp. 347-360.

SOLOVE D.J., « Privacy and power : Computer Databases and Metaphors for Information Privacy », *Stanford L.R.*, 2001, vol. 53, pp. 1395-1462.

SOLOVE J.D., « A taxonomy of privacy », *Univeristy of ¨Pennsylvania Law Review,* 2006, pp. 477-560.

SOLOVE D.J., « 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy », *San Diego Law review*, vol. 44, 745, 2007, pp. 745-772.

SPF FEDICT, « Étude longitudinale d'Internet et de l'e-government en Belgique. La parole au citoyen. Enquête réalisée par Indigov à la demande de Fedict », *Fed-eView Citizen*, 2006.

SUMMERS R., « Toward a better general theory of legal validity », *Rechtstheorie Berlin,* 1985, pp. 67-83.

TATON X. et VAN DER HAEGEN O., « Le droit européen des recours juridictionnels en matière de régulation : un recul de l'autonomie procédurale des États membres », *J.D.E.,* 2011, pp. 157-166.

TENE O., « Privacy : The new generations », *International Data Privacy Law,* 2011, pp. 15 et s.

TCHANG-BENOIT C., « Les atteintes aux droits individuels par l'usage abusif des techniques de l'informatique et rôle de l'avocat dans l'organisation d'une protection de la personne contre les dangers de l'ordinateur », *Gaz. Palais,* 1973, pp. 226-230.

THEUNIS J., « De 'exceptie van onwettigheid' (artikel 159 G.W.) : meer vragen dan antwoorden ? », *R.W.,* 2007-2008, pp. 1266 à 1281.

THEUNIS J., « Le principe de la confiance légitime dans la jurisprudence de la Cour constitutionnelle », *R.B.D.C.*, 2008/1, pp. 5-22.

THIELEMANS R., « Grondrechten en de bevoegdheden van staat, gemeenschappen en gewesten. Openbaarheid van bestuur, motivering van bestuurhandelingen en ombudsman », *T.B.P.,* 1990, pp. 438-448.

TOURNEPICHE A.-M., « Vers de nouveaux champs d'application pour la transparence administrative en droit communautaire », *C.D.E.,* 2007, liv. 5-6, pp. 623-646.

TROPER M., « Le concept d'État de droit », *Droits*, 1992, pp. 51 et s.

TRUDEL P., « Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau », mars 2003, 52 pages disponibles sur http://www.chairelrwilson.ca/cours/drt6929d/egouvMRCI23-06.pdf

TRUDEL P., « Renforcer la protection de la vie privée dans l'état en réseau : l'aire de partage des données personnelles », *Revue française d'administration publique*, 2004/2, n° 110, pp. 257-266.

TRUDEL P., « Chapter 7. The Development of Canadian Law with respect to E-government » *in Designing e-Government* (dir. J.E.J. PRINS), Kluwer Law International, 2007, pp. 113-164

TRUDEL P., « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *Revista catalana de dret public,* num. 35, 2007, pp. 247-280.

UYTTENDAELE M., « Fédéralisme et libertés fondamentales : la transparence administrative au regard de la réforme de l'État », *A.P.T.*, 1993, pp. 96-105.

VAN BULCK K., « La Commission de la protection de la vie privée etle Comité de surveillance institué auprès de la Banque Carrefour : répartition des tâches relatives au secteur de la sécurité sociale », *Rev. b. séc. Soc.*, 1993, pp. 327-339.

VANDEN BERGHE L., « Légalité et illégalité dans les échanges de renseignements entre administrations fiscales belges », *R.G.F.,* 1987, pp. 174 et s.

VAN EECKHOUTTE D., « Luchtruim is niet exclusief federaal, Noordzee ook niet », *Juristenkrant*, 2007, p. 7.

VAN KRIEKINGE D., « La Banque-Carrefour des Entreprises en tant que pilier de l'e-gouvernement : un pas vers la simplification administrative ? », *R.D.T.I.,* 2004, pp. 7-23.

VAN DROOGHENBROECK S., « La loi du 25 février 2003 tendant à lutter contre la discrimination. Les défis d'une 'horizontalisation' des droits de l'homme », *A.P.T.,* 2003, pp. 208-252.

VAN OVERSTRAETEN M. et DEPRÉ S., « Le traitement automatisé de données à caractère personnel et le droit au respect de la vie privée en Belgique », *R.T.D.H.,* 2003, pp. 665 à 701.

VELAERS J. et VANPRAET J., « De materiële en territoriale bevoegdheidverdeling inzake sociale zekerheid en sociale bijstand », *T.B.P.*, 2008, pp. 323-345.

VELAERS J. et VAN DROOGHENBROECK S., « Note relative à l'insertion d'une clause constitutionnelle transversale sur les compétences en matière de garantie et de restriction des droits fondamentaux dans le cadre du régime fédéral belge », *Doc. Parl.,* Chambre, session 2004-2005, Doc 51 2304/001, pp. 1 -206.

VERDEGEM P. ET HAUTTEKEETE L., »(M)E-Government : Elektrische diensten op de maat van de burger », *Bb & b,* 2007, pp. 258-272.

VERDUSSEN M., « La signification du principe de l'État de droit pour l'administration en Europe », *in X. Verfassungsprinzipien in Europa, Constitutional principles in Europa, Principes constitutionnels en Europe* (dir. H. BAUER et C. CALLIES), Athènes, Berlin, Bruxelles, Ant. N. Sakkoulas, Berliner wissenschaft-verlag, Bruylant, 2008, pp. 189-218.

VERDUSSEN M. et NOËL A., « Les droits fondamentaux et la réforme constitutionnelle de 1993 », *A.P.T.,* 1994, pp, 127-143.

VULLIET-TAVERNIER S., « Après la loi du 6 août 2004 : nouvelle loi 'informatique et libertés', nouvelle CNIL ? », *Droit social*, 2004, pp. 1055-1065.

WALLEMACQ A., « Le registre national des personnes physiques », *J.T.,* 1984, pp. 701-706.

WATHELET M., « Principe de proportionnalité : utilisation disproportionnée ? », *J.T.,* 2007, pp. 313-316.

ZARKA Y.-C., « Internet ou la révolution paradoxale », *Cités,* 2009/3, n° 39, pp. 3-6.

* * *

Table des matières

Préface 7

Remerciements 13

Sommaire 17

Introduction générale 19

Prélude 29

Introduction 31

CHAPITRE I. L'e-gouvernement 33

Introduction 33

Section 1. Des techniques nouvelles 38

I. De nouveaux outils 38

A. La source authentique de données 39

B. La plateforme d'échanges d'informations 46

C. Le numéro d'identification 61

II. De nouvelles opérations 67

A. L'octroi d'avantages aux citoyens : l'automatisation des droits 68

B. Le contrôle des citoyens : le profilage 72

Section 2. Des craintes nouvelles 83

I. Un déséquilibre important entre l'administration et les citoyens 85

II. La normalisation des comportements 91

III. La technocratie 95

IV. Les failles dans la sécurité informatique 97

Conclusions 100

CHAPITRE II. La protection de la vie privée et des données à caractère personnel 103

Introduction 103

Section 1. Le lien entre la protection des données à caractère personnel et la protection de la vie privée 104

I. La protection des données à caractère personnel : un outil au service d'une valeur, la vie privée 105
A. Des règles pour protéger le libre développement personnel face aux technologies 105
B. Des règles enracinées dans le droit fondamental à la protection de la vie privée 109
II. La protection des données à caractère personnel : un régime juridique spécifique 114
Section 2. Les notions cardinales de la protection des données à caractère personnel 121
I. La donnée à caractère personnel 121
II. Le traitement de données 122
III. Le responsable du traitement 124
Conclusions 127
Conclusions du prélude 129

Titre I. La légalité de l'e-gouvernement 131
Introduction 133
CHAPITRE I. L'e-gouvernement et l'exigence constitutionnelle de légalité 135
Introduction 135
Section 1. L'e-gouvernement et le législateur compétent 137
I. Les décrets et les ordonnances soumis à la loi du 8 décembre 1992 138
II. Une solution insatisfaisante 140
Section 2. L'e-gouvernement et la compétence du législateur 144
I. La raison d'être de l'exigence de légalité confrontée à l'e-gouvernement 145
A. La raison d'être de la loi 145
B. La raison d'être de la loi ébranlée par l'e-gouvernement 149
II. La densité de l'exigence de légalité dans l'e-gouvernement 158
A. L'intervention du législateur 158
B. L'intervention du Roi 168
Conclusions 175

CHAPITRE II. L'e-gouvernement et les exigences de finalité et de proportionnalité des traitements de données à caractère personnel 177

Introduction 177

Section 1. L'exigence de finalité 178

I. Une finalité légitime 180

II. Une finalité déterminée 184

A. L'exigence de finalité confirme le principe de spécialité 185

B. L'exigence de finalité renforce le principe de spécialité 187

III. Une finalité explicite 192

IV. Une finalité compatible 194

A. Les « dispositions légales et réglementaires » et les « prévisions raisonnables de l'intéressé » 198

B. La finalité compatible précisée par le législateur 203

Section 2. L'exigence de proportionnalité 209

I. La proportionnalité du traitement 213

A. Un traitement de données est-il nécessaire ? 213

B. Le traitement de données réalise-t-il un équilibre entre le but poursuivi et l'immixtion dans la vie privée ? 218

II. La proportionnalité des données 225

A. La qualité des données 226

B. La limitation des données 228

Conclusions 235

CHAPITRE III. L'organisation d'un e-gouvernement légal 237

Introduction 237

Section 1. La structure de l'e-gouvernement 238

I. Les impératifs 239

A. La protection de la vie privée et le concept de Privacy by design 239

B. L'efficacité administrative et la circulation des données 241

II. Le choix du modèle de l'État en réseaux 252

Section 2. L'encadrement législatif de l'e-gouvernement 254

I. Des lois particulières 256

A. Les plateformes d'échanges d'informations 258

B. Les sources authentiques de données 267

C. Les numéros d'identification 273

II. Une loi-cadre 282
A. Le modèle et les définitions 284
B. Les exigences de finalité et de proportionnalité applicables aux données et aux traitements 285
C. Les règles applicables à l'administration demanderesse des données 287
D. Les règles applicables à l'administration émettrice des données 288
E. Le contrôle de l'échange de données au sein d'un réseau et entre réseaux 290
III. Des accords de coopération 295
A. La justification des accords de coopération dans l'e-gouvernement 295
B. Les caractéristiques des accords de coopération dans l'e-gouvernement 298
Conclusions 306
Conclusions du Titre I 309

Titre II. La transparence de l'e-gouvernement 311
Introduction 313
CHAPITRE I. L'e-gouvernement et la transparence administrative 315
Introduction 315
Section 1. La notion de transparence administrative 315
I. L'émergence de la transparence administrative 315
A. L'origine de la transparence administrative 316
B. La raison d'être de la transparence administrative 318
II. Le contenu de la transparence administrative 321
A. Le droit de savoir : la publicité des documents administratifs 322
B. Le droit de comprendre : la motivation formelle des actes administratifs 325
Section 2. Le droit de savoir ébranlé par l'e-gouvernement 326
I. La publicité passive confrontée à l'e-gouvernement 327
A. La demande d'accès 328
B. La réponse de l'autorité 356
II. La publicite active confrontée à l'e-gouvernement 373
A. Des obligations limitées 373
B. Des améliorations nécessaires 375

Section 3. Le droit de comprendre ébranlé par l'e-gouvernement 383
I. L'acte à motiver 384
II. Le contenu de la motivation 386
Conclusions 395
CHAPITRE II. L'e-gouvernement et la transparence des traitements de données à caractère personnel 399
Introduction 399
Section 1. La notion de transparence des traitements de données à caractère personnel 399
I. La raison d'être de la transparence des traitements de données à caractère personnel 400
II. Le contenu de la transparence des traitements de données à caractère personnel 402
Section 2. La publicité passive des traitements de données à caractère personnel 403
I. La procédure d'accès aux données à caractère personnel 404
A. Le droit d'accès 404
B. Les limitations du droit d'accès 409
II. Une procédure d'accès à simplifier 411
A. Les embûches 412
B. Des pistes de solution 414
Section 3. La publicité active des traitements de données à caractère personnel 420
I. L'obligation d'information 420
A. Le principe de l'obligation d'information 421
B. Les exceptions à l'obligation d'information 427
II. L'obligation de déclaration 431
A. Le principe de l'obligation de déclaration 431
B. Les exceptions à l'obligation de déclaration 434
Conclusions 440
CHAPITRE III. L'organisation d'un e-gouvernement transparent 443
Introduction 443
Section 1. Des impératifs 443
I. L'organisation de la convergence et de la complémentarité des règles 444
II. L'actualisation des règles 447
A. La loi du changement 448

B. Le principe de la réciprocité des avantages 450
Section 2. Des solutions 455
I. L'accès à une vue d'ensemble de l'administration 458
A. L'index des documents généraux pertinents 459
B. Le panorama de la structure administrative 460
C. Le cadastre des interconnexions 461
II. L'accès à une vue individualisée de l'administration 466
A. Le répertoire des références 467
B. L'*audit trail* 468
Conclusions 474
Conclusions du Titre II 475

Titre III. Le contrôle de l'e-gouvernement 477
Introduction 479
CHAPITRE I. L'e-gouvernement et le contrôle organisé par le droit administratif 481
Section 1. Les contrôles juridiques 482
I. Le contrôle par les autorités non juridictionnelles 483
A. Les autorités médiatrices 483
B. Les autorités consultatives 490
II. Le contrôle par les autorités juridictionnelles 504
A. Le contrôle par la Cour constitutionnelle et le Conseil d'État 504
B. Le contrôle par les juridictions judiciaires 520
Section 2. Le contrôle politique 537
I. Les objectifs du contrôle politique de l'e-gouvernement 538
II. Les embûches du contrôle politique de l'e-gouvernement 539
Conclusions 542
CHAPITRE II. L'e-gouvernement et le contrôle organisé par le régime juridique de la protection des données à caractère personnel 545
Section 1. Le contrôle à l'initiative de la personne concernée 545
I. Les droits de rectification, d'opposition et d'interdiction 546
A. L'utilité des droits de rectification, d'opposition et d'interdiction 547
B. La difficulté d'exercer les droits de rectification, d'opposition et d'interdiction dans l'e-gouvernement 550

II. Le dépôt de plainte 552
III. Le recours « comme en référé » devant le Tribunal de première instance 556
A. L'utilité du recours 557
B. La difficulté d'exercer le recours dans l'e-gouvernement 558
IV. L'action en réparation 560

Section 2. Le contrôle par la CPVP 562
I. Le statut de la CPVP 565
A. Une autorité de régulation 566
B. Une autorité indépendante ? 573
C. Une autorité légitime ? 584
II. Les moyens d'action de la CPVP 618
A. Le contrôle des traitements de données en projet : les avis 619
B. Le contrôle des traitements de données en cours : les recommandations et les autorisations 625
C. Le contrôle des traitements de données contestés : la gestion des plaintes, le pouvoir d'enquête, le pouvoir de dénonciation et le pouvoir d'ester en justice 645

Section 3. Le contrôle par le détaché à la protection des données 651
I. Le rôle du détaché à la protection des données 651
II. L'intérêt d'instituer un détaché à la protection des données dans chaque administration 656
A. L'amélioration de la protection des données à caractère personnel 656
B. L'allègement des formalités administratives 660

Conclusions 662

CHAPITRE III. L'organisation d'un e-gouvernement contrôlé 665

Section 1. Le renforcement de l'indépendance et de la légitimité de la CPVP 666
I. Le renforcement de l'indépendance de la CPVP 666
A. L'indépendance des membres de la CPVP 667
B. L'indépendance institutionnelle de la CPVP 670
II. Le renforcement de la légitimité de la CPVP 671
A. Organiser le contrôle politique de la CPVP 671
B. Organiser le contrôle juridictionnel et la transparence de la CPVP 680

Section 2. Le renforcement de l'efficacité de la CPVP 689
I. Un renforcement de la mission d'information 691
II. Un renforcement des moyens de contrôle de la CPVP 694
A. La dénonciation des traitements illégaux dans le rapport annuel 695
B. L'octroi d'un pouvoir d'injonction, d'un pouvoir d'admonestation et d'un pouvoir d'amende 697
C. La capacité de saisir la Cour constitutionnelle et le Conseil d'État 707
D. La suppression des comités sectoriels 708
Conclusions 713

Conclusions du Titre III 715

Conclusions générales 717
I. L'enrichissement du droit administratif 718
II. Le rééquilibrage du droit administratif 721

Bibliographie 729

Table des matières 749