Le R.G.P.D., les lois belges et le secteur public

DEGRAVE, ELISE

Published in:
Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.)

Publication date:
2020

Document Version
le PDF de l'éditeur

6

LE R.G.P.D., LES LOIS BELGES ET LE SECTEUR PUBLIC

Les traitements de données dans l'administration en réseaux et l'Autorité de protection des données

Élise DEGRAVE

chargée de cours à l'UNamur
directrice de recherche au Centre de Recherche Information, Droit et Société – CRIDS

Sommaire

Introduction

L'étude de la mise en œuvre du R.G.P.D. au sein du secteur public invite à se pencher sur la structure et le fonctionnement de l'administration dite « électronique », que l'on appelle aussi « e-gouvernement ». De profonds bouleversements se sont opérés dans ce secteur, à la faveur du déploiement, au sein des services, d'outils numériques d'un genre nouveau, destinés à maximiser les échanges de données à caractère personnel des citoyens.

Il s'agira ensuite, dans le cadre de cette étude consacrée au secteur public, de mettre en lumière une institution publique clé pour la protection des données, à savoir, l'Autorité de protection des données, qui a succédé depuis peu à la Commission de la protection de la vie privée.

On espérait que le R.G.P.D. uniformise les règles de protection des données au travers de l'Europe et en facilite la lecture. Dans le secteur public belge, c'est l'effet contraire qui est observé puisque l'entrée en application du R.G.P.D. s'est accompagnée de l'adoption – jusqu'ici – de quatre nouvelles législations, venues remplacer, compléter, ou modifier des normes déjà éparses et complexes[1].

Ainsi, la loi du 3 décembre 2017 est consacrée à l'Autorité de protection des données, qui remplace la Commission de la protection de la vie privée.

La loi du 30 juillet 2018 précise les aspects du R.G.P.D. à propos desquels une marge de manœuvre était laissée aux législateurs nationaux[2].

La loi du 5 septembre 2018 institue le Comité de sécurité de l'information[3].

Enfin, la loi du 25 novembre 2018 opère une réforme importante de la loi sur le Registre national[4].

À l'occasion de cette contribution, les éléments pertinents de ces différentes législations sont analysés dans la mesure où ils sont nécessaires pour comprendre la mise en œuvre du R.G.P.D. dans les administrations et le fonctionnement de l'Autorité de protection des données.

1 Pour aider les personnes concernées dans les méandres des règles applicables au secteur public, nous avons initié deux ouvrages collectifs dédiés à cette thématique : É. Degrave (dir.), *L'ABC du R.G.P.D. Dictionnaire pratique à destination des administrations*, Namur, U.V.C.W., 2018 ; C. de Terwangne et É. Degrave (dir.), *La protection des données à caractère personnel en Belgique. Manuel de base*, Bruxelles, Politeia, 2019.

2 Ci-après, « loi-cadre ».

3 Ci-après, « loi C.S.I. ».

4 Ci-après, « loi R.N. ».

Section 1

Les traitements de données à caractère personnel au sein du secteur public

A. L'objectif de collecte unique des données et l'administration en réseaux

Depuis plusieurs années, on assiste à une simplification administrative évidente. Nombre de démarches administratives peuvent désormais être effectuées en quelques clics depuis un ordinateur ou un smartphone, épargnant tant aux citoyens qu'aux administrations, les files d'attente aux guichets, la constitution sans erreur de dossiers papier, de nombreux courriers d'échange d'informations, etc.

Par exemple, l'application « e-birth » permet désormais aux hôpitaux d'envoyer l'attestation de naissance sous format électronique aux communes, leur permettant d'enclencher rapidement les procédures administratives conséquentes à cet événement.

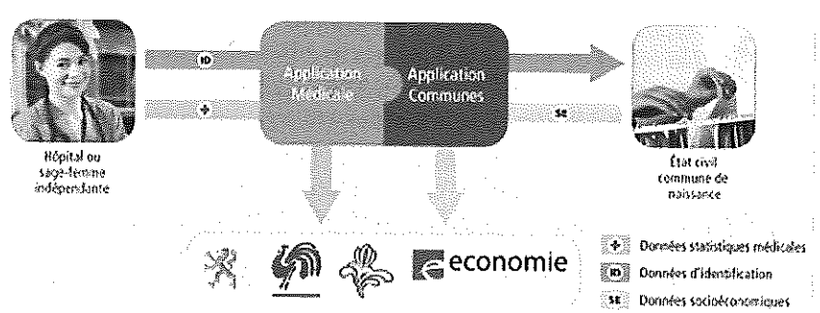
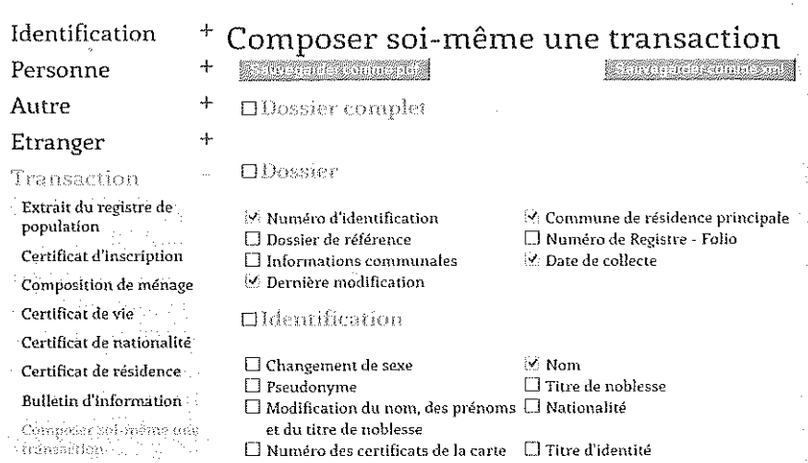


Schéma du fonctionnement de l'application e-birth, disponible sur le site www.ehealth.fgov.be/fr/esante/professionnels-de-la-sante/ebirth/en-savoir-plus

Autre exemple, le citoyen peut désormais obtenir en ligne, sur le site du Registre national, des documents personnels et officiels qui nécessitaient jadis un déplacement à la commune. Ces documents sont générés en PDF, assortis de la signature électronique, et ont la même force probante que le même document obtenu à la commune, comme l'affirme l'article 4 de la loi du 8 août 1983 sur le Registre national.



Extrait du portail « Mon dossier » du Registre national, comprenant la liste des documents officiels pouvant être obtenus via cet outil, ainsi que la possibilité de composer soi-même un document en sélectionnant les informations à y faire figurer

Progressivement, les portails de simplification administrative se multiplient, comme en témoigne le site www.mybelgium.be. On y trouve le lien vers différentes applications de service public, tels que tax-on-web (déclaration fiscale en ligne), mypension (calcul de la pension), mycareer (aperçu détaillé de la carrière), myminfin (dossier fiscal en ligne), etc., qui sont tous opérationnels.

Si cette simplification administrative est désormais possible, c'est parce que la structure de l'administration a été bouleversée par la mise en place, en son sein, d'outils numériques d'un genre nouveau. Cette structure a été tout à fait repensée en fonction d'un objectif majeur : la collecte unique des données (1). Il s'en est suivi la mise en place d'une administration dite « en réseaux » (2).

1. L'objectif de la collecte unique des données

À la base de l'administration électronique et de sa structure particulière qui sera analysée ci-après se trouve un objectif fort : celui de la collecte unique des données. Il s'agit de ne demander qu'une seule fois aux citoyens les informations qui les concernent, à la différence de ce qui se faisait jadis, lorsque les individus devaient communiquer, à répétition, leurs mêmes données à chaque administration avec laquelle ils étaient en contact. En d'autres termes, aujourd'hui, 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.

En pratique, il est nécessaire que la collecte unique soit soutenue par la mise en place d'un système qui permette la réutilisation des données fournies

initialement, et donc leurs échanges 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.

L'objectif de collecte unique des données et la nécessaire réutilisation de celles-ci entre les administrations ne sont pas que des vœux pieux. Ces impératifs sont consacrés par plusieurs textes normatifs, notamment une loi du 5 mai 2014 qui soumet l'ensemble des S.P.F. fédéraux à l'obligation de collecte unique de données[5].

C'est pourquoi, la structure et le fonctionnement de l'administration sont aujourd'hui organisés dans l'idée de rendre possibles la collecte unique des données et la réutilisation des informations entre les administrations[6].

2. Le passage d'administrations en silos à une administration en réseaux

Jadis, les institutions publiques œuvraient de manière cloisonnée, chacune indépendamment l'une de l'autre. Elles collectaient auprès des citoyens les informations dont elles avaient besoin pour l'exécution de leurs propres missions et ne les partageaient pas ensuite. On peut ainsi affirmer que l'administration était structurée « en silos ».

Il en résultait une perte de temps et d'argent pour l'administration, qui devait contacter chaque personne pour chaque information nécessaire, attendre sa réponse, réclamer éventuellement des précisions, mais aussi pour le citoyen qui était contraint de communiquer de multiples fois la même information aux institutions gérant un dossier à son sujet, d'effectuer des démarches administratives qui impliquaient d'identifier l'administration compétente, de se déplacer, de respecter des horaires stricts et de prendre patience dans les files d'attente.

Avec l'apparition des technologies, on constate que les administrations peuvent désormais collaborer efficacement. La volonté naît alors d'encourager les « synergies entre les divers services et niveaux des pouvoirs publics »[7], dans le but de simplifier les démarches et procédures administratives. La technologie rend aisé et rapide l'échange des informations relatives aux citoyens. Cela permet notamment d'alléger les tâches administratives des citoyens, en automati-

5 Voy. loi du 5 mai 2014 « garantissant le principe de collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier », *M.B.*, 4 juin 2014.

6 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.

7 Commission de la protection de la vie privée (ci-après, « C.P.V.P. »), 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, n° 5.

sant l'octroi de certaines allocations, par exemple, et de renforcer l'efficacité de l'administration, en améliorant la lutte contre la fraude, notamment[8].

Pour mettre en œuvre efficacement l'échange des informations entre administrations, la Belgique s'engage, depuis plusieurs années, dans un modèle d'administration inédit, qui consiste à mettre en place des réseaux d'administrations au sein desquels un intégrateur de services assure l'échange des données entre les administrations concernées.

Le modèle d'administration en réseaux a devancé, en l'incarnant avant l'heure, la concrétisation du concept de «*privacy by design*», l'un des principes importants du R.G.P.D.[9], qui veut que l'on tienne compte de la protection de la vie privée dès l'étape de conception de l'outil. C'est exactement ce souci de protection de la vie privée dans l'architecture même du modèle d'administration qui a présidé au choix d'organiser l'administration en réseaux. Dans le même temps, cette préoccupation a poussé à renoncer au modèle de centralisation des données, évoqué par exemple au moment du projet «SAFARI» en France, qui faisait craindre notamment un grand risque de piratage des données facilité par le fait que l'ensemble des données aurait été disponible en un point unique[10].

En pratique, comment ce modèle se concrétise-t-il précisément? Dans un premier temps, les administrations ayant un point commun (p. ex., un objet de travail commun ou l'appartenance à une même entité, fédérale ou fédérée) sont regroupées au sein d'un ensemble appelé «réseau».

Ensuite, différentes administrations se voient attribuer la responsabilité de collecter, enregistrer et mettre à jour certaines données déterminées. Les bases de données contenant ces informations et placées chacune sous la responsabilité d'une administration sont appelées «sources authentiques de données». L'idée est de faire en sorte que chaque information relative au citoyen ne soit enregistrée qu'une seule fois par une seule administration du réseau, qui est ensuite responsable de la fiabilité de ces données.

Enfin, on place, au cœur de ce réseau d'administrations, un outil d'un type nouveau : l'intégrateur de services, dit aussi «plate-forme d'échange d'informations» ou encore «Banque-carrefour». En somme, l'intégrateur de services est une infrastructure technique, placée au cœur d'un réseau d'administrations, et qui est chargée d'assurer, au sein de ce réseau, l'échange électronique d'informations provenant de sources authentiques diverses. Ainsi, lorsqu'une administration a besoin d'une donnée dont elle ne dispose pas, il lui suffit de s'adresser à l'intégrateur de services qui contacte l'administration détentrice de la donnée recherchée et l'achemine ensuite vers l'administration qui la lui a demandée.

Afin de faciliter la compréhension de l'exposé, on peut schématiser comme suit le modèle d'un réseau d'administrations comprenant un intégrateur de services.

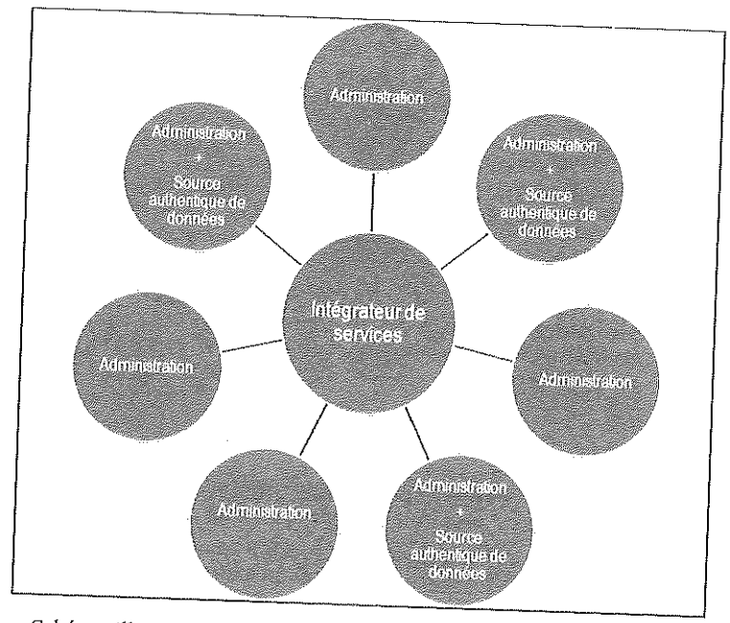


Schéma illustrant un réseau d'administrations composé d'un intégrateur de services auquel sont reliées plusieurs administrations dont certaines détiennent une source authentique de données

Depuis quelques années, plusieurs réseaux d'administrations ont progressivement été créés au sein du secteur public belge. Ils comprennent chacun, en leur cœur, un intégrateur de services.

Historiquement, le premier réseau du genre est le réseau de la sécurité sociale, qui regroupe les institutions de sécurité sociale et au sein duquel œuvre la Banque-carrefour de la sécurité sociale. Ce réseau et cet intégrateur de services sont en place depuis le début des années 1990[11].

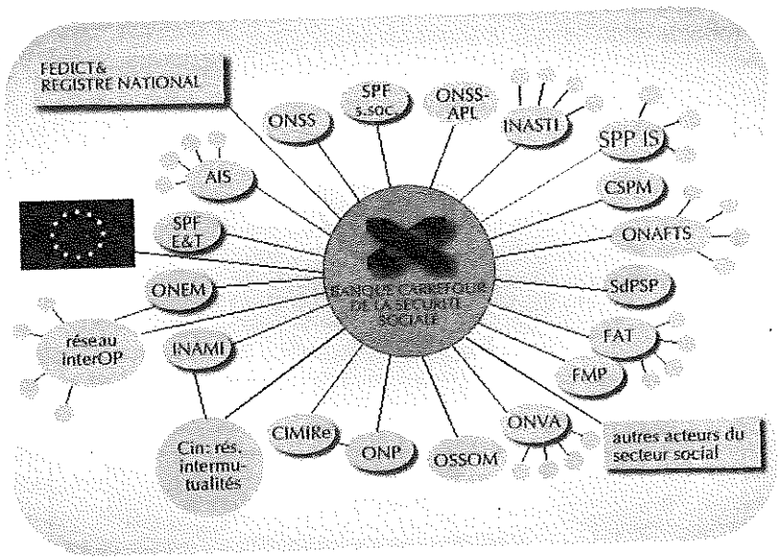
8 Pour de plus amples développements sur l'e-gouvernement et le modèle de l'administration en réseaux, voy. D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen*, Bruges, Vanden Broele, 2005, pp. 1 à 13 ; É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, coll. CRIDS, Bruxelles, Larcier, 2014, en particulier nos 172 et s.

9 Art. 25 R.G.P.D.

10 À ce sujet, voy. É. Degrave, «Opportunités et risques du numérique pour le citoyen usager des services publics», *in* H. Jacquemin et M. Nihoul (dir.), *Vulnérabilités et droits dans l'environnement numérique*, coll. Faculté de droit, Bruxelles, Larcier, 2018, pp. 551 et s.

11 Voy. 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 du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale».

Depuis lors sont apparus d'autres réseaux, tels que notamment le réseau sectoriel de la santé, au sein duquel la plate-forme *eHealth* assume le rôle d'intégrateur de services[12] ou le réseau des véhicules avec en son cœur la Banque-carrefour des véhicules[13].



Exemple d'intégrateur de services : la Banque-carrefour de la sécurité sociale, placée au cœur du réseau de la sécurité sociale

La structure de l'administration en réseaux présente de nombreux avantages en termes d'efficacité administrative. Mais elle crée aussi des difficultés à plusieurs égards. Deux difficultés retiennent particulièrement notre attention, compte tenu de leur importance dans un État de droit et des solutions que le R.G.P.D. et les lois belges tentent d'y apporter. Il s'agit, d'une part, de la transparence des traitements de données et, d'autre part, de leur contrôle.

B. La transparence des traitements de données et l'exercice du droit d'accès (art. 15 R.G.P.D.)

Il n'est plus possible, pour un citoyen, de « mettre la main » sur son dossier administratif. Celui-ci n'existe plus. Les données, désormais numériques et donc intangibles, sont aussi éparpillées entre les différentes sources authentiques de l'administration.

12 Voy. la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme *eHealth* et portant diverses dispositions, *M.B.*, 13 octobre 2008.

13 Loi du 19 mai 2010 portant sur la création de la Banque-carrefour des véhicules, *M.B.*, 28 juin 2010.

Dans ce contexte, comment, par exemple, vérifier que les données utilisées par l'administration pour juger de l'octroi d'une allocation ou décider d'un contrôle fiscal sont correctes ? Où faire rectifier des données inexactes qui apparaîtraient, par exemple, sur un avertissement extrait de rôle ? Étant donné que les données traitées dans le contexte de l'e-gouvernement ont vocation à être réutilisées un grand nombre de fois, pour pouvoir réaliser l'objectif de collecte unique des données, une erreur affectant une donnée aura un effet domino, et sera démultipliée autant de fois que la donnée aura été réutilisée. Il est donc impératif de pouvoir rapidement supprimer les erreurs l'affectant. Or, ce n'est pas chose aisée. À cet égard, à propos de l'utilisation d'une donnée à caractère personnel erronée dans une décision administrative, le médiateur fédéral a affirmé il y a quelques années que « trouver où et comment l'erreur a été commise revient presque à chercher une aiguille dans une botte de foin »[14]. Le constat n'a malheureusement pas changé depuis lors.

C'est ici qu'apparaît la force et l'utilité du droit à la transparence des données à caractère personnel, c'est-à-dire le droit de chacun de connaître les éléments importants qui concernent le traitement de ses données, tels que les informations collectées à son sujet, par quoi, pour combien de temps et pour quelles raisons[15].

Après avoir établi les fondements du droit à la transparence (1), l'étude se penche sur l'exercice de ce droit en pratique (2).

1. Les fondements du droit à la transparence

Le droit à la transparence des données est un corollaire au *droit fondamental à la protection de la vie privée* des citoyens. Le droit fondamental à la vie privée, consacré par l'article 22 de la Constitution, s'entend aujourd'hui d'un droit à l'autodétermination informationnelle. En d'autres termes, chacun a le droit de décider lui-même de l'utilisation de ses données à caractère personnel ou, au moins[16], d'avoir connaissance de l'usage qui en est fait[17]. C'est pourquoi, en l'occurrence, il importe que chaque citoyen puisse avoir une vision claire des bases de données dans lesquelles sont et seront enregistrées les informations

14 Médiateur fédéral, *Rapport annuel 2010*, p. 90.

15 Voy. *infra*.

16 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 communiquées et enregistrées à défaut de quoi, le citoyen n'aurait pas d'existence civile.

17 Dans le même sens, H. BURKERT, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *in 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* F. Rigaux (dir.), *La vie privée : une liberté parmi les autres ?*, Bruxelles, Larcier, 1992, pp. 231 et s. ; R. LEENES et B.-J. KOOPS, « "Code" and privacy or how technology is slowly eroding privacy », *in* E. Dommering et L. Asscher (dir.), *Coding regulation. Essays on the Normative Role of Information technology*, La Haye, TMC Asser Press, 2006, pp. 143 et 144.

qu'il est contraint de donner à l'administration. Dans le même temps, le respect de cet impératif favorise la confiance du citoyen en l'État. Le fait de savoir ce que l'État détient comme données et par quelle administration ces données sont conservées apaise, d'une part, les peurs liées à l'existence d'un État « *Big Brother* », qui saurait tout de tout le monde et, d'autre part, les craintes que l'usage des technologies dans le secteur public provoque le développement d'une administration kafkaïenne, c'est-à-dire une administration à ce point opaque et complexe qu'on ne parvient plus à la comprendre et la contrôler[18].

La transparence sous-tend le *régime juridique de la protection des données organisé par le R.G.P.D.* D'une part, aux articles 13 et 14, le R.G.P.D. consacre le droit de chacun d'être informé, au moment de la collecte des données, d'un certain nombre d'éléments relatifs au traitement (identité du responsable du traitement, finalités du traitement, destinataires des données, etc.). D'autre part, en son article 15, le R.G.P.D. consacre le droit de la personne concernée d'accéder aux données traitées à son sujet et aux éléments qui entourent ces traitements (finalités du traitement, destinataires des données, etc.) mais aussi le droit d'en obtenir gratuitement une copie. Ce droit d'accès et de copie est particulièrement important, car il est la porte d'entrée vers les autres droits consacrés par le R.G.P.D. que sont les droits de rectification, d'effacement et d'opposition visés aux articles 16 et suivants.

Par ailleurs, s'agissant des données traitées par l'administration, on ne peut faire fi du droit fondamental à la *transparence administrative*, consacré par l'article 32 de la Constitution et organisé, au niveau fédéral, par loi du 11 avril 1994 relative à la publicité de l'administration[19] et par décrets dans les entités fédérées[20]. Cette dernière impose à l'administration des obligations de publicité active qui consistent à fournir, d'initiative, « une information claire et objective sur l'action des autorités administratives fédérales »[21]. En ce sens, la Charte des services publics impose d'ailleurs clairement aux services publics de recourir aux technologies pour s'adapter aux besoins du public, en affirmant 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 »[22].

Enfin, au-delà de la transparence pour le citoyen désireux de connaître l'usage qui est fait de ses propres données et de pouvoir les corriger le cas échéant, l'impératif de transparence est également nécessaire pour rendre tout

18 Au sujet de ces craintes, voy. É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, nos 61 et s.

19 Loi du 11 avril 1994 relative à la publicité de l'administration.

20 Décret flamand du 18 mai 1999 relatif à la publicité de l'administration ; décret de la Communauté française du 26 mars 2004 relatif à la publicité de l'administration ; décret de la Communauté germanophone du 16 octobre 1995 relatif à la publicité des documents administratifs.

21 Art. 2 de la loi du 11 avril 1994.

22 Charte de l'utilisateur des services publics du 4 décembre 1992, *M.B.*, 22 janvier 1993, Partie I, Chapitre II, Section 2.

à fait effective *l'obligation légale de collecte indirecte des données*. En particulier, il faut que les cours et tribunaux, eux aussi, puissent voir clair sur quel type de donnée est enregistré dans quelle base de données. Il faut, en effet, que les juges puissent vérifier si, dans un cas particulier, la donnée était bien disponible dans le réseau, auquel cas l'administration était obligée de trouver cette donnée par elle-même ou si, dans l'hypothèse où cette donnée n'était pas disponible dans le réseau, l'administration pouvait la collecter directement auprès du citoyen. Une telle vérification suppose que les juges aient eux aussi connaissance des types de données et de leur localisation.

2. L'exercice en pratique du droit d'accès consacré à l'article 15 du R.G.P.D.

On l'a dit, le droit de chacun d'accéder aux données qui le concernent et qui sont détenues par le responsable du traitement est une prérogative essentielle pour comprendre la manière dont l'administration traite les données des citoyens, mais aussi pour exercer le droit de chacun d'obtenir la rectification et l'effacement de ses données, ou s'opposer à leur utilisation future. Pourtant, à l'heure actuelle et bien que le droit d'accès aux données existe en Belgique depuis plus de vingt-cinq ans[23], il demeure peu connu du public et peu exercé.

Après avoir testé l'exercice de ce droit dans le cadre de nos recherches, on peut raisonnablement penser que son ineffectivité est liée à la lourdeur et à la complexité de sa concrétisation. De toute évidence, à l'heure actuelle, 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, encore faut-il pouvoir authentifier ce courriel[24], ce qui requiert, par exemple, une signature électronique. Une fois la demande introduite, il est contraint de patienter, l'administration disposant d'un mois pour répondre[25].

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.

23 Ce droit était déjà consacré par la loi du 8 décembre 1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel.

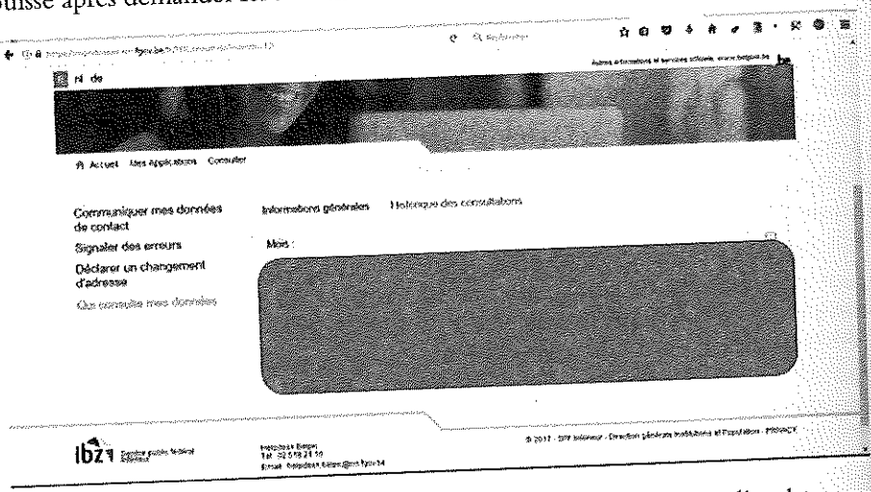
24 Cons. 57 R.G.P.D.

25 Art. 12.3 R.G.P.D.

Néanmoins, dans le parcours semé d'embûches que représente la demande d'accès d'un citoyen à ses données à caractère personnel, on aperçoit un outil très bien pensé et éminemment pragmatique. Il s'agit de l'outil « Mon dossier » du Registre national[26].

Cet outil a été créé il y a plus de dix ans par le S.P.F. Intérieur, qui gère le Registre national. Chaque citoyen peut y accéder en ligne. Après s'être identifié avec sa carte d'identité électronique, il accède à un portail qui lui permet de voir l'ensemble de ses données enregistrées au Registre national. Un onglet lui permet de signaler les erreurs affectant ses données, le cas échéant.

Le citoyen peut aussi cliquer sur l'onglet « Qui consulte mes données », et voir apparaître le nom des institutions s'étant intéressées à lui, dans l'idée qu'il puisse après demander les raisons de telles consultations et en vérifier la légalité.



Extrait du portail « Mon dossier » du Registre national contenant l'onglet « qui consulte mes données »

Étant donné la grande utilité de cet outil dans le contexte de l'e-gouvernement, tant pour alléger la démarche du citoyen exerçant son droit d'accès que la lourde tâche qui s'impose à l'administration chargée de répondre à ce citoyen, il est urgent de généraliser l'outil « Mon dossier » du Registre national et de le mettre en place pour l'ensemble des sources authentiques de données.

Concrètement, en consultant le portail internet dédié à l'administration électronique, le citoyen devrait pouvoir s'identifier avec sa carte d'identité électronique et voir apparaître la liste de toutes les sources authentiques de données

26 Lien vers l'outil : www.ibz.rrn.fgov.be/fr/registre-national/mon-dossier/.

qui contiennent des données à son sujet. En cliquant dessus, il pourrait consulter ces données, comme il peut le faire pour le Registre national.

Il faudrait également mettre en place un « audit trail », c'est-à-dire un outil permettant de tracer les échanges de données entre les différentes administrations. De telles informations peuvent être très intéressantes lorsqu'il s'agit, par exemple, de trouver la source d'une erreur affectant une donnée et de prévenir chaque institution l'ayant utilisée[27].

Ce sont des pistes pour lesquelles nous plaidons depuis longtemps déjà. À la faveur de l'entrée en application du R.G.P.D., notamment, la situation dans ce domaine a l'air de progresser depuis peu. Récemment, l'Office de la transformation digitale du S.P.F. Stratégie et Appui a créé un portail internet dénommé www.passezaudigital.be. On y annonce la création d'un portail web pour les administrations. L'explication, encore fort vague, affirme qu'il s'agit d'« une application qui permet aux différentes institutions fédérales d'enregistrer les données comme l'exige le R.G.P.D. ». On y annonce également que « par la suite, les citoyens européens pourront également consulter ce portail web pour voir les données dont dispose le gouvernement à leur sujet, à quelles fins ces données sont utilisées et de quelle manière ils peuvent faire exercer leurs droits, par exemple le droit à l'oubli ou le droit à la portabilité des données »[28]. Espérons qu'il s'agira là d'une réelle mesure de transparence et d'information au bénéfice des citoyens et qu'elle sera effectivement suivie en pratique.

C. Le contrôle spécifique des traitements de données au sein de l'administration

On l'a dit, les échanges de données au sein de l'administration en réseaux sont nombreux, du fait de la réutilisation maximale des données collectées de manière unique auprès des citoyens. Mais comment s'assurer que les échanges de données effectués respectent les exigences du R.G.P.D. ?

Durant très longtemps, le contrôle des échanges de données entre administrations a été effectué par des organes de la C.P.V.P. appelés « comités sectoriels ». Leur rôle était d'autoriser, ou de refuser, le transfert des données détenues par l'État. De cette manière, chaque source authentique de données était protégée par un comité sectoriel spécifique. Ainsi, le comité sectoriel Registre national contrôlait l'usage fait des données enregistrées dans la source authentique

27 Pour plus de détails à propos de la mise en place d'une vue individualisée de l'administration, voy. É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, n^os^ 396 et s.

28 www.passezaudigital.be/actualites/la-mise-en-conformite-avec-le-RGPD-simplifiee-grace-un-nouveau-portail-web.

« Registre national »[29], le comité sectoriel de la sécurité sociale et de la santé contrôlait les données enregistrées dans les sources authentiques des administrations œuvrant en matière de sécurité sociale et de santé[30], le comité sectoriel de la Banque-carrefour des entreprises contrôlait les données de la Banque-carrefour des entreprises[31], etc. Certes, ces comités sectoriels étaient critiquables notamment en ce que leur indépendance n'était pas garantie[32]. Mais ils avaient le mérite de jouer le rôle de « chien de garde » des sources de données authentiques détenues par l'État, en agissant, en principe, de manière cohérente avec les avis et les positions de la Commission vie privée. En d'autres termes, face à l'incapacité du législateur et du gouvernement d'anticiper la multitude des traitements de données au sein de l'administration, les comités sectoriels constituaient un relais qui, sur le terrain, veillait, en principe, au respect des normes, au cas par cas. En outre, les décisions des comités sectoriels étaient publiques.

Au moment de l'adoption de la loi A.P.D., le législateur a décidé de supprimer les comités sectoriels[33], sans indiquer par quoi ils seraient remplacés. Il s'avère à présent que ce contrôle a été remplacé par des mesures parcellaires, sans cohérence.

Ce contrôle est organisé de manière disparate, par le R.G.P.D., mais aussi par la loi-cadre, la loi A.P.D., la loi C.S.I. et la loi R.N.[34].

Ces contrôles spécifiques sont au nombre de trois. La rédaction de protocoles, visés à l'article 20 de la loi-cadre, est le contrôle de principe. Pour certains types de données, le législateur a opté pour un mécanisme de contrôle différent, ce qui n'aide pas à la lisibilité et la compréhension de la matière. Ainsi, les données du Registre national, les données de sécurité sociale et de santé font l'objet d'un contrôle particulier.

On remarquera d'emblée le manque de cohérence de ces réformes successives et parcellaires qui eurent dû plutôt être menées concomitamment. Alors que la loi A.P.D. a supprimé les comités sectoriels, arguant notamment de la lourdeur des procédures d'autorisation, la loi réformant le Registre national fait resurgir la procédure d'autorisation préalable en en donnant les clés au ministre

29 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 C.P.V.P.

30 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.

31 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 C.P.V.P.

32 À ce sujet, voy. É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, n^os^ 492 et s.

33 Voy. art. 109 de la loi A.P.D.

34 Nous nous concentrons ici sur le rôle des organes spécifiquement dédiés au contrôle des traitements de données au sein de l'administration. Pour le contrôle effectué par les juridictions judiciaires ainsi que par la Cour constitutionnelle et le Conseil d'État, voy. C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base*, *op. cit.*, pp. 154 et s.

de l'Intérieur, tandis que la loi sur le Comité de sécurité de l'information va jusqu'à ressusciter tant la procédure d'autorisation préalable que le comité sectoriel supprimé quelques mois plus tôt.

Dressons à présent les traits majeurs de ces nouveaux contrôles spécifiques de l'administration en analysant à cet égard le rôle du protocole (1), du ministre de l'Intérieur (2) et du Comité de sécurité de l'information (3).

1. Le protocole pour contrôler les échanges de données émanant d'une autorité publique fédérale

Le protocole est un document dont la rédaction est imposée par la loi-cadre qui met en œuvre le R.G.P.D. en Belgique, mais non par le R.G.P.D. lui-même.

Les lignes qui suivent détaillent les modalités et les caractéristiques de ces protocoles.

a) Les hypothèses dans lesquelles un protocole doit être rédigé

Le protocole doit, en principe, être obligatoirement rédigé lorsque deux conditions cumulatives sont remplies.

Premièrement, il faut identifier l'origine des données. En effet, le protocole est obligatoire lorsque les données utilisées proviennent d'une *autorité publique fédérale*.

Par exemple, lorsqu'une commune demande la communication de données détenues par l'Administration générale de la documentation patrimoniale – qui fait partie du S.P.F. Finances – en vue d'octroyer les permis d'urbanisme, un protocole doit être rédigé avant que cette autorité publique fédérale transfère les données demandées.

Deuxièmement, il faut veiller à ce que l'une des *trois bases de finalités* suivantes fonde le transfert envisagé : l'article 6.1, c) (le traitement est nécessaire au respect d'une obligation légale), l'article 6.1, d) (le traitement est nécessaire à la sauvegarde des intérêts vitaux d'une personne physique), ou l'article 6.1, e) (le traitement 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). Dans ces cas, un protocole doit obligatoirement être établi.

Il ne peut être fait exception à l'obligation de rédiger un protocole que si des lois particulières le prévoient. Notons qu'il ressort des travaux préparatoires de cette loi[35] qu'un tel protocole ne doit pas être rédigé pour les flux internes à la police intégrée au sens de l'article 2, 2°, de la loi du 7 décembre 1998, sans

35 Exposé des motifs du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 44.

toutefois que cette exception soit explicitement affirmée dans ladite loi. Enfin, les travaux préparatoires de cette loi font également état du fait qu'un protocole ne doit pas être rédigé pour « des flux de et vers l'étranger » au motif que l'article 1.3 du R.G.P.D. affirme que « la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ».

b) *La raison d'être du protocole*

La rédaction d'un protocole répond à deux objectifs.

Le premier objectif est celui de la *responsabilisation* des responsables du traitement, dans l'esprit du R.G.P.D. et du principe d'« *accountability* ». Étant donné que les comités sectoriels ont été supprimés, il revient désormais aux responsables du traitement impliqués dans un transfert de données d'examiner eux-mêmes la légalité du transfert envisagé et de fixer, par écrit, les modalités de celui-ci.

Le deuxième objectif est celui de la *transparence* vis-à-vis du public. L'idée est de formaliser le transfert de données dans un document pour en garder une trace et le publier. À nouveau, puisque les comités sectoriels – dont les autorisations étaient jadis accessibles au public en ligne – ont été supprimés, il était nécessaire de trouver une autre voie pour rendre publics ces transferts de données dans l'administration.

Malheureusement, telle qu'elle est organisée actuellement par la loi-cadre, la publicité des protocoles ne nous semble pas suffisante pour atteindre cet objectif[36].

c) *Les auteurs du protocole*

L'obligation de rédiger un protocole dans les hypothèses précitées repose sur le responsable du traitement de l'autorité publique fédérale émettrice des données et sur le responsable du traitement destinataire des données, qui peut être soit une autorité publique, soit une entreprise.

Une fois rédigé, le protocole doit être soumis à l'avis du délégué à la protection des données (« D.P.O. ») de l'autorité émettrice des données et à l'avis du délégué à la protection des données du destinataire des données. Ces avis doivent être annexés au protocole.

Les responsables du traitement ne sont pas obligés de suivre ces deux avis. Néanmoins, si au moins l'un des deux avis n'est pas suivi, le protocole doit être

36 Voy. *infra*.

complété afin de mentionner, en introduction, « la ou les raisons pour laquelle ou lesquelles ce ou ces avis n'ont pas été suivis »[37].

Remarquons que seuls les responsables de traitement rédigent ce protocole, et ne sont même pas contraints de suivre l'avis des D.P.O. L'article 20 de la loi-cadre semble inspiré du mécanisme des « ententes de partage »[38] pratiqué au Canada, à la grosse différence près qu'au Canada, ces ententes doivent être validées par l'autorité de contrôle. Le législateur n'a pas voulu instaurer pareil contrôle. Il s'agit là pour nous d'un recul inquiétant dans la protection des données des citoyens.

En effet, on ne le dira jamais assez, les données qui émanent de l'État sont à manier avec précaution : ce sont des données relatives à tous les citoyens, qui touchent à maints aspects de leur vie (situation familiale, situation fiscale, habitation, véhicule, etc.). Les citoyens n'ont pas le choix : ils sont obligés de les fournir à l'État. De plus, ainsi qu'on l'a évoqué précédemment, vu que l'administration est fondée sur l'obligation de collecte unique des données, les transferts de données émanant des autorités publiques sont donc la règle et leur réutilisation est maximale. Il importe donc d'autant plus que des garanties suffisantes soient mises en place pour éviter tout abus dans l'usage de ces données, qui auraient de graves conséquences sur la confiance du citoyen en l'état, à l'heure du déploiement des outils numériques.

En l'occurrence, on doit donc s'inquiéter que les échanges de données provenant des sources authentiques de l'État soient désormais protégés de manière si légère. Non seulement il n'y a plus, sur ces échanges, de contrôle des comités sectoriels, mais en plus, ces échanges font l'objet d'un accord entre responsables du traitement, en dehors de tout contrôle de l'A.P.D. et sans que les mentions à y indiquer soient obligatoires[39]. Dans la foulée, on doit redouter aussi que des chantages émergent entre responsables de traitement, qui consisteraient à conditionner l'envoi de telles données à la réception de telles autres. Il en va d'autant plus ainsi que l'hypothèse où les responsables de traitement ne s'entendraient pas sur les conditions du protocole n'est absolument pas abordée par la loi. En outre, il y a un risque de voir réapparaître les pratiques illégales qui existaient avant la mise en place de comités sectoriels où, à défaut de procédure claire, il arrivait que des agents de l'administration s'accordent entre eux sur l'envoi de certaines données qui étaient ensuite envoyées par mail non sécurisé. De tels transferts se faisaient en toute opacité, faisant fi de tout examen juridique. De simples protocoles non contrôlés par l'A.P.D. ne risquent-ils pas de recréer pareilles dérives[40] ?

37 Art. 20, § 2, *in fine*.

38 À ce sujet, voy. art. 67 et s. de la loi canadienne sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ; É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, nos 222 et s.

39 *Cf.* point suivant.

40 Dans le même sens, voy. S.L.C.E., avis n° 63.192/2 du 19 avril 2018, préc., n° 54-3126/001, pp. 422 et s.

d) *Le contenu du protocole*

La loi donne une liste d'éléments qui peuvent être intégrés au protocole en vue d'en faire apparaître clairement les éléments essentiels et les différentes modalités, de manière à répondre à l'objectif de responsabilisation et de transparence précité. Cette liste est exemplative, non limitative. Il n'est pas exclu que d'autres éléments soient ajoutés au protocole. Que du contraire, d'ailleurs. Au moment de la rédaction d'un protocole, il est utile d'avoir en tête le double objectif de responsabilisation des protagonistes et de transparence vis-à-vis du citoyen. Tout élément permettant d'atteindre au mieux ces objectifs est donc le bienvenu.

Ainsi, l'article 20, § 1er, alinéa 2, énonce les éléments suivants :

« Ce protocole peut prévoir notamment :

1° l'identification de l'autorité publique fédérale qui transfère les données à caractère personnel et celle du destinataire ;
2° l'identification du responsable du traitement au sein de l'autorité publique qui transfère les données et au sein du destinataire ;
3° les coordonnées des délégués à la protection des données concernés au sein de l'autorité publique qui transfère les données ainsi que du destinataire ;
4° les finalités pour lesquelles les données à caractère personnel sont transférées ;
5° les catégories de données à caractère personnel transférées et leur format ;
6° les catégories de destinataires ;
7° la base légale du transfert ;
8° les modalités de communication utilisée ;
9° toute mesure spécifique encadrant le transfert conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut ;
10° les restrictions légales applicables aux droits de la personne concernée ;
11° les modalités des droits de la personne concernée auprès du destinataire ;
12° la périodicité du transfert ;
13° la durée du protocole ;
14° les sanctions applicables en cas de non- respect du protocole, sans préjudice du titre 6 ».

À cela doi(ven)t s'ajouter, comme précité, la ou les raisons pour laquelle ou lesquelles le ou les avis des délégués à la protection des données n'ont pas été suivis, le cas échéant.

En tout cas, tout en regrettant que le législateur n'ait pas rendu ces éléments de contenu obligatoires, on ne peut qu'encourager les responsables du traitement à faire figurer au minimum ces éléments-là dans leur protocole.

Notons qu'il serait particulièrement utile que l'A.P.D. propose, sur son site internet, un modèle type de protocole qui pourrait, tout à la fois, aider les responsables du traitement impliqués dans les transferts de données concernés mais

également faciliter la tâche de l'A.P.D. lorsqu'elle sera amenée à contrôler ces traitements de données.

e) *La publication du protocole*

Le protocole doit être publié sur le site internet de chaque responsable du traitement concerné par le transfert de données.

Initialement, le gouvernement n'avait prévu aucune mesure de publicité, ce qui a fait réagir la section de législation du Conseil d'État. Celle-ci a affirmé qu'« étant donné que ces protocoles organisent une ingérence dans la vie privée, ils doivent être accessibles pour les personnes concernées en vertu de l'article 22 de la Constitution de manière à assurer la prévisibilité des transferts et des traitements. Or, le protocole ne bénéficie pas de la publicité réservée à la loi qui lui sert de base légale et cette dernière, par nature, ne contient pas les éléments essentiels du transfert qui sont contenus dans le protocole. Dès lors, il s'impose que les protocoles soient publiés »[41]. La C.P.V.P. est même allée plus loin, soutenant qu'« afin d'assurer la prévisibilité des flux de données visés, ces protocoles d'échange devront faire l'objet d'une publication au *Moniteur belge* [...]. Dans la mesure où ces protocoles vont encadrer les traitements de données des citoyens, ils doivent répondre aux critères de prévisibilité et d'accessibilité[42] »[43].

À la suite de ces remarques, le gouvernement a ajouté à la disposition concernée que le protocole serait publié sur le site internet des responsables de traitement concernés.

Nous déplorons cette solution. Compte tenu du nombre d'institutions concernées, de la qualité très variable de leur site internet dont certains ne sont pas à jour ou particulièrement fastidieux à lire, on doute fort que pareille mesure aide tout qui le souhaite à prendre connaissance et comprendre sans trop de difficultés les traitements de données opérés par les autorités publiques fédérales. Il aurait été bien plus judicieux de centraliser pareille publicité sur le site internet de l'A.P.D. en les classant selon un critère clair qui pourrait être lié au type de données traitées.

41 S.L.C.E., avis n° 63.192/2 du 19 avril 2018, préc., n° 54-3126/001, p. 424.

42 *Cf.*, à ce sujet, C.J.C.E., 1er octobre 2015, affaire *Smaranda Bara*, ECLI:EU:C:2015:638 ; Cour eur. D.H., 4 décembre 2015, affaire *Roman Zakarov c. Russie*, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160008%22]}.

43 C.P.V.P., avis n° 33/2018 du 11 avril 2018 sur un avant-projet de loi « relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, pp. 782 et 783, n° 162.

2. L'autorisation du ministre de l'Intérieur pour contrôler les données du Registre national

Le Registre national est le « coffre-fort » des Belges. Cette source authentique de données est encadrée par loi du 8 août 1983 organisant un registre national des personnes physiques[44].

Chaque citoyen est enregistré au Registre national dès sa naissance. Il reçoit alors un « numéro d'identification au Registre national »[45] qui est unique[46]. Ce numéro est signifiant, sa lecture permettant de connaître la date de naissance et le sexe de la personne. Le N.I.R.N. constitue aussi le numéro fiscal, permettant l'accès aux données fiscales de la personne, ainsi que le numéro de sécurité sociale, permettant l'accès aux données de sécurité sociale et de santé de l'individu concerné. Un précieux sésame donc.

En vertu de l'article 3 de la loi R.N., pour chaque citoyen, entre 13 et 17 données sont enregistrées au Registre national[47]. À ces données légales s'ajoutent des « types d'information » (dits « T.I. ») qui précisent ces données légales[48].

Les données du Registre national ont une valeur unique dans l'administration, car, en principe[49], 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.

Jusqu'ici, l'accès aux données du Registre national et leur utilisation étaient clairement et strictement encadrés par la loi du 8 août 1983. Entre autres balises, le traitement des données du Registre national devait être autorisé par le Comité sectoriel du Registre national, après une analyse des éléments essentiels de ces traitements au regard notamment des exigences de proportionnalité et de finalité des traitements envisagés. Par ailleurs, les entreprises privées ne pouvaient accéder à ces informations, ni utiliser le N.I.R.N. Les institutions y habilitées, limitativement énumérées par l'article 5 de la loi R.N., étaient essentiellement des autorités publiques ou des institutions chargées d'exécuter des tâches d'intérêt général[50].

44 Ci-après, « loi R.N. ».

45 Ci-après, « N.I.R.N. ».

46 Voy. arrêté royal du 3 avril 1984 « relatif à la composition du numéro d'identification des personnes inscrites au Registre national des personnes physiques ». Pour de plus amples détails à ce sujet, voy. K. Rosier, « Le numéro d'identification du registre national : une donnée pas comme les autres », *Bull. soc.*, 2007, p. 6 ; É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os 29 et s.

47 Il s'agit notamment des nom, prénom, date de naissance, filiation, profession, état civil, composition de ménage, situation de séjour des étrangers, etc.

48 La liste des types d'informations enregistrés au Registre national est disponible ici www.ibz.rrn.fgov.be/fr/registre-national/reglementation/instructions/liste-des-types-dinformation/. Par exemple, le T.I. 004 mentionne le changement de sexe du citoyen, le T.I. 111 indique le statut juridique de la personne telle qu'une minorité prolongée par exemple.

49 Nous nuançons notre propos dans la mesure où, pour l'heure, de nombreux duplicata des données d'identification des citoyens existent dans les administrations, ce qui devrait changer à l'avenir.

La loi du 25 novembre 2019 « portant des dispositions diverses concernant le Registre national et les registres de population » a apporté de profondes et peu heureuses modifications à cette situation.

Cela faisait quelques années déjà que Jan Jambon souhaitait assouplir les règles balisant l'usage des données du Registre national et notamment, ouvrir le Registre national aux entreprises privées[51]. De toute évidence, la suppression des comités sectoriels lui a facilité la tâche.

Plusieurs modifications ont ainsi été introduites dans la loi R.N. Deux d'entre elles retiennent notre attention dans le cadre de cette étude : le pouvoir d'autorisation confié au ministre de l'Intérieur et l'ouverture du Registre national aux entreprises privées.

a) Le pouvoir d'autorisation confié au ministre de l'Intérieur

Le comité sectoriel Registre national ayant été supprimé, la loi confie désormais au ministre de l'Intérieur le pouvoir d'autoriser l'accès aux données du Registre national ainsi que l'utilisation du N.I.R.N.[52]. Mais ce n'est pas tout. Ce ministre peut déléguer ce pouvoir « au fonctionnaire responsable de l'administration en charge de la gestion du Registre national des personnes physiques les missions qui lui incombent [...] », comme l'indique l'article 28 de la loi R.N.

Entre autres craintes[53], étant donné que ce pouvoir est désormais confié à une personne seule, on peut raisonnablement se demander s'il n'y a pas là un danger que des pressions s'exercent sur le ministre ou le fonctionnaire responsable du Registre national pour obtenir l'accès aux données ou l'autorisation d'utiliser le précieux sésame que représente le N.I.R.N. et que ces précieuses données soient donc divulguées au mépris des impératifs de protection des données des citoyens.

Plus encore, la loi R.N. organise maintes exceptions à l'obligation de demander l'autorisation d'utiliser le N.I.R.N.[54]. Cela signifie donc que le N.I.R.N. peut être utilisé sans contrôle préalable et en toute opacité. On peut alors raisonnablement craindre que s'opère une banalisation de ce numéro, avec tous les risques ainsi engendrés compte tenu du fait que, rappelons-le, le

50 Pour plus d'informations à ce sujet, voy. Bruxelles (9e ch.), 9 mai 2012, *J.T.*, 2012, pp. 691 à 693, obs. É. Degrave, « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données illégal sanctionné par la Cour d'appel de Bruxelles » ; C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base, op. cit.*, pp. 169 et s.

51 Cette intention était déjà dénoncée en 2017. Voy. P. Havaux, « Vie privée : le coffre-fort des Belges bientôt percé », 19 janvier 2017.

52 Art. 5 et 8, § 2, de la loi R.N.

53 Pour plus de détails, voy. C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base, op. cit.*, pp. 173 et s.

54 Art. 8, §§ 1er, 5 et 7, de la loi R.N.

N.I.R.N. est aussi le numéro fiscal et le numéro de sécurité sociale, permettant d'accéder à de nombreuses bases de données.

b) *L'ouverture du Registre national au secteur privé*

Alors que les données du Registre national étaient jadis réservées essentiellement aux autorités publiques ou des institutions chargées d'exécuter des tâches d'intérêt général, *les associations de fait et les personnes physiques* ont désormais accès au Registre national. Les *entreprises* voient également leur pouvoir étendu dans ce domaine.

1° L'accès au Registre national des associations de fait et des personnes physiques

L'article 5, § 1er, 2°, de la loi R.N. prévoit désormais que *les associations de fait et les personnes physiques* ont accès au Registre national.

À la suite des critiques de la C.P.V.P. jugeant cette ouverture beaucoup trop large[55], le législateur a suivi les recommandations faites par l'autorité de contrôle et a ajouté que cet accès était possible pour les associations de fait et les personnes physiques « expressément *habilitées par* une loi, un décret ou une ordonnance à connaître les informations nécessaires à l'accomplissement de *missions d'intérêt général qui leur sont confiées par ou en vertu*[56] d'une loi, d'un décret ou d'une ordonnance ». Il était en effet impératif de ne pas ouvrir le Registre national aux associations de fait et aux personnes physiques sans autre condition. La question demeure toutefois de savoir quels sont, finalement, les cas visés par cette hypothèse et s'il était donc nécessaire de l'intégrer dans la loi.

Il n'en demeure pas moins que deux aspects importants de l'accès au Registre national n'ont pas été déterminés par le législateur, malgré l'avis de la C.P.V.P. très explicite à ce sujet.

D'une part, on constate un recul dans les mesures de sécurité qui entourent le traitement des données du Registre national.

En effet, malgré les demandes très précises de la C.P.V.P. à cet égard, le législateur n'a pas défini les mesures de sécurité adéquates que les utilisateurs du Registre national doivent mettre en place. Non seulement, cela n'aide pas lesdits utilisateurs qui demeurent dans le flou quant aux exigences requises, mais cela met également en péril la sécurité de ces précieuses données.

De plus, depuis la loi du 25 novembre, les utilisateurs du Registre national ne sont plus tenus de désigner nominativement ceux de leurs organes ou

55 C.P.V.P., avis n° 106/2018 du 17 octobre 2018, avis d'initiative – Audition de l'Autorité de protection des données sur le projet de la loi portant des dispositions diverses concernant le Registre national et les registres de population – Doc. 54 3256 – Suivi de l'avis 19/2018 de la C.P.V.P. (CO-A-2018-132), *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3256/003, pp. 5 et 6.

56 C'est nous qui soulignons.

préposés qui disposent d'un accès au Registre national. Comme l'a souligné la C.P.V.P., « aucune justification n'est reprise dans l'exposé des motifs quant à cette suppression alors que cette obligation oblige les utilisateurs du Registre national à limiter les membres de leur personnel habilités à consulter le Registre national au strict nécessaire »[57]. Il y a là également un recul dans les garanties devant limiter les abus dans l'utilisation des données.

D'autre part, on regrette que le législateur n'ait pas veillé à trouver une cohérence entre cette loi et l'article 20 de la loi-cadre détaillé précédemment, qui organise la conclusion de protocole pour tout transfert de données émanant d'une source authentique de l'État, comme l'est le Registre national. Cette demande avait également été formulée par la C.P.V.P.[58] mais n'a pas été suivie par le législateur. De toute évidence, cette lacune créera des difficultés en pratique.

2° La communication automatique des données du Registre national aux entreprises privées

L'article 5*ter* de la loi R.N. affirme que, désormais, certaines données du Registre national (nom, résidence principale et décès) et leur mise à jour pourront être communiquées automatiquement aux entreprises privées, moyennant le consentement de la personne concernée.

Heureusement, les nombreuses remarques de la C.P.V.P.[59] ne sont pas passées inaperçues et plusieurs balises sont aujourd'hui fixées. Ainsi, les finalités de la mise à jour des données par les entreprises privées sont détaillées, le consentement clair de la personne concernée est exigé, il est explicitement affirmé que ces données ne peuvent pas être réutilisées à des fins publicitaires. Par contre, là aussi, le législateur a refusé de préciser les mesures de sécurité qui devraient être mises en place au sein de ces entreprises[60].

Toutefois, une question fondamentale demeure : était-ce réellement nécessaire d'ouvrir le Registre national aux entreprises privées, pour la seule mise à jour de l'adresse et la mention du décès ? Cette mesure n'est-elle pas disproportionnée, en ce que les risques ainsi créés sont plus nombreux que les avantages que l'on peut retirer de pareille mesure ?

Certes, la loi R.N. balise l'usage de ces données. Mais cela ne garantit pas que, concrètement, ces balises seront respectées par les responsables de traitement. Comment s'assurer, par exemple, que la mise à jour de l'adresse d'un client que l'entreprise détient pour la finalité « facturation » ne va pas ensuite être réutilisée à des fins de marketing ? Disposant de la donnée « adresse » mise à jour, on doute fort que, pour sa publicité, l'entreprise utilise l'ancienne adresse…

57 C.P.V.P., avis n° 106/2018 du 17 octobre 2018, préc., p. 115, n° 11.

58 *Ibid.*, p. 6.

59 C.P.V.P., avis n° 19/2018, préc., pp. 206 et s.

60 C.P.V.P., avis n° 106/2018, préc., p. 113, n° 9.

Pourra-t-on identifier rapidement les entreprises qui encourageraient les clients à donner leur consentement contre un bon de réduction, ce qui est interdit ? Par ailleurs, comment le citoyen lui-même pourra-t-il identifier les abus ? L'accès à ses données par les entreprises privées sera-t-il indiqué dans l'outil « Mon dossier », rubrique « qui a consulté mes données » ? Comment pourra-t-il exercer son droit d'opposition ? Il y a beaucoup de risque que, *de facto*, le respect des balises légales ne puisse être vérifié.

Par ailleurs, puisque les services du Registre national devront envoyer les mises à jour des données à certaines sociétés avec lesquelles la personne concernée a conclu un contrat, cela signifie que ces services connaîtront, pour chacune de ces personnes, les sociétés auprès desquelles elles ont conclu un contrat. Cela rentre-t-il dans les missions d'une administration d'avoir connaissance de ces éléments privés ?

En somme, cette modification législative signifie donc que l'objectif de simplification administrative annoncé par le ministre provoque, concrètement, un risque d'abus dans l'usage des données, une plus grande intrusion dans la vie privée des citoyens et une plus lourde charge pour le citoyen qui souhaite rester informé de l'usage qui est fait de ses données et qui devra effectuer des démarches pour ce faire[61].

Ainsi donc, au vu de l'importance des données du Registre national, et, en particulier, du N.I.R.N., il est inquiétant que les balises légales jusqu'ici claires et strictes aient été assouplies en faveur des entreprises privées, pour des objectifs peu clairs, qui ne convainquent pas du caractère proportionné des traitements de données à venir dans le secteur privé.

3. Le Comité de sécurité de l'information pour contrôler les données de sécurité sociale et de santé

Le Comité de sécurité de l'information[62] a été créé par la loi du 5 septembre 2018[63]. Cette dernière modifie deux lois importantes en matière d'e-gouvernement, à savoir la loi du 15 janvier 1990 relative à la Banque-carrefour

61 À ce sujet, voy. P. Havaux, « Le Registre national, un "indic" des boîtes privées pour accéder aux données des Belges. La vie privée n'est pas assez protégée », *Le Vif-L'Express*, 29 novembre 2018.

62 Ci-après, « C.S.I. ».

63 Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE, *M.B.*, 10 septembre 2018. Ci-après, « loi C.S.I. ».

de la sécurité sociale[64] et du 15 août 2012 qui concerne l'intégrateur de services fédéral[65].

Disons-le d'emblée : le C.S.I. est un comité sectoriel ressuscité[66]. Il a été créé par le législateur pour jouer le même rôle que les comités sectoriels que ce même législateur avait supprimés quelques mois plus tôt. Cette situation schizophrénique souligne encore un peu plus le manque de cohérence dans les législations qui ont suivi l'entrée en application du R.G.P.D.

Les lignes qui suivent font état, de manière très synthétique, des traits majeurs du C.S.I., s'agissant de sa composition, de ses compétences et du contrôle de ses décisions[67].

a) La composition du C.S.I.

Le C.S.I. est composé de deux chambres, la chambre « sécurité sociale et santé » et la chambre « autorité fédérale ». Ces chambres siègent en « chambres réunies » dans certains dossiers.

Parmi les huit membres effectifs du C.S.I., on retrouve des experts en sécurité informatique, en protection des données, en gestion des identités électroniques, des juristes spécialisés en droit social ou de la santé et des médecins spécialisés en gestion des données santé[68]. Leur mandat est de six ans, renouvelable.

Dans l'exercice de leurs missions, ils ne peuvent recevoir d'instructions de personne et ne peuvent relever de l'autorité hiérarchique des ministres de tutelle de cette institution[69].

b) Les compétences du C.S.I.

Pour l'essentiel, le C.S.I. œuvre de la même manière que l'ex-comité sectoriel « sécurité sociale et santé » et l'ex-comité sectoriel « autorité fédérale ».

Ainsi, la chambre « sécurité sociale et santé » du C.S.I. est compétente pour autoriser, ou refuser, la communication de données sociales qui émane d'une institution de sécurité sociale ou de la Banque-carrefour de la sécurité sociale. En fonction de l'institution destinatrice de ces données, la chambre « autorité

64 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, p. 3288.

65 Loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, *M.B.*, 29 août 2012.

66 À ce sujet, voy. la contribution de L. Gérard, *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base*, *op. cit.*, pp. 174 et s.

67 Pour de plus amples précisions à ce sujet, voy. la contribution très détaillée de L. Gérard, *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base*, *op. cit.*, pp. 174 et s.

68 Art. 2 de la loi C.S.I.

69 Pour plus de détails, voy. art. 3 et 4 de la loi C.S.I.

fédérale» doit également se joindre à la décision, pour rendre une décision en «chambres réunies»[70].

La chambre «autorité fédérale» quant à elle n'intervient que de manière subsidiaire. Elle autorise, ou refuse, la communication de données à caractère personnel qui émanent d'un service public ou d'une institution publique fédérale, dans l'hypothèse seulement où les autorités concernées par cette communication de données ne parviennent pas à s'entendre sur un protocole d'échange de données[71] ou si l'une de ces autorités souhaite obtenir pareille décision du C.S.I.[72].

c) *Le contrôle des décisions du C.S.I.*

L'une des critiques importantes adressées jadis aux comités sectoriels résidait dans le flou qui entourait le contrôle de leurs décisions pourtant contraignantes[73]. Cette situation incertaine était notamment liée au statut peu clair de la C.P.V.P. et de ces organes décisionnels institués en son sein[74].

Qu'en est-il aujourd'hui? Est-il possible de contester voire d'obtenir l'annulation d'une décision du C.S.I.? Il convient de répondre par l'affirmative, car les décisions du C.S.I. sont susceptibles d'être contrôlées par l'Autorité de protection des données et par la section du contentieux administratif du Conseil d'État.

1° Le contrôle des décisions du C.S.I. par l'A.P.D.

Le contrôle des décisions du C.S.I. par l'A.P.D. n'était pas prévu initialement dans l'avant-projet de loi. On peut donc se réjouir que, sur ce point, tant les remarques pertinentes de la C.P.V.P.[75] que celles de la section de législation du Conseil d'État[76] aient été suivies.

Désormais, ce contrôle est organisé par les articles 46, § 2, de la loi du 15 janvier 1990 et 35/1, § 2, de la loi du 15 août 2012[77]. Il est toutefois regrettable, comme l'a souligné la C.P.V.P.[78], que ce contrôle n'ait pas plutôt été intégré dans la loi A.P.D., ce qui aurait permis de gagner en cohérence et en simplicité…

70 Pour plus de détails sur ces hypothèses, voy. art. 18 de la loi C.S.I.

71 *Cf. supra.*

72 Art. 86 de la loi CSI.

73 Voy. É. Degrave, «La Commission de la protection de la vie privée : un organisme invincible ?», obs. sous Cour administrative du Grand-Duché du Luxembourg, 12 juillet 2005, *R.D.T.I.*, 2006, pp. 225 à 241.

74 À ce sujet, voy. É. Degrave, *L'e-gouvernement et la protection de la vie privée*, *op. cit.*, n°s 489 et s.

75 Commission pour la protection de la vie privée, avis n° 34/2018 du 11 avril 2018, p. 4.

76 Projet de loi instituant le comité de sécurité de l'information […], Avis de la section de législation du Conseil d'État n° 63.202/2, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 130.

77 C.P.V.P., avis n° 34/2018 du 11 avril 2018 relatif à la demande d'avis concernant un avant-projet de loi instituant le comité de sécurité de l'information […], p. 4.

78 C.P.V.P., avis n° 34/2018 préc., p. 4.

Ainsi donc, ainsi que l'affirme la loi, l'Autorité de protection des données peut examiner la légalité d'une décision du C.S.I. au regard des normes juridiques supérieures. Elle peut le faire «à tout moment», ce qui suppose donc qu'elle puisse agir soit d'initiative, soit à la suite d'une plainte ou d'une requête portée auprès d'elle par une personne concernée.

Si l'A.P.D. constate une illégalité, elle doit le faire «de manière motivée». Ensuite, elle peut demander au C.S.I. de «reconsidérer cette délibération sur les points qu'elle a indiqués, dans un délai de quarante-cinq jours et exclusivement pour le futur»[79], sans autre précision, notamment sur la réaction qui devrait être celle de l'A.P.D. en cas de refus du C.S.I. de revoir sa décision. Le caractère peu incisif des termes utilisés et le manque de précision évoqué peuvent faire craindre une faible effectivité de cette disposition à l'avenir[80].

2° Le contrôle par le Conseil d'État, section du contentieux administratif

Bien que la loi C.S.I. ne le mentionne pas explicitement, les décisions du C.S.I. sont susceptibles de faire l'objet d'un recours en annulation devant le Conseil d'État, section du contentieux administratif.

En effet, le C.S.I. répond aux critères de l'autorité administrative[81] au sens de l'article 14 des lois coordonnées sur le Conseil d'État[82]. De plus, les travaux préparatoires la loi C.S.I. affirment explicitement l'existence de pareil recours, que ce soit dans l'exposé des motifs qui mentionne «les procédures de recours existantes auprès du Conseil d'État» ou le commentaire des articles du projet de loi qui indique que «les délibérations sont publiées […] et peuvent être contestées par les voies de recours applicables (comme un recours auprès du Conseil d'État)»[83].

Conformément à la procédure habituelle devant le Conseil d'État, le recours en annulation, auquel pourrait être jointe une demande de suspension[84], doit être formé dans les soixante jours suivant la publication de la délibération sur les sites internet utilisés par le Comité de sécurité de l'information[85].

79 Art. 46, § 2, de la loi du 15 janvier 1990 et art. 35/1, § 3, de la loi du 15 août 2012.

80 En ce sens, L. Gérard, *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base*, *op. cit.*, p. 185.

81 Voy. *ibid.*, pp. 187 et s.

82 Lois sur le Conseil d'État, coordonnées le 12 janvier 1973, *M.B.*, 21 mars 1973.

83 Projet de loi instituant le comité de sécurité de l'information […], *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, pp. 10 et 31.

84 Art. 17 des lois coordonnées.

85 Art. 4 de l'arrêté du Régent du 23 août 1948 déterminant la procédure devant la section du contentieux administratif du Conseil d'État, *M.B.*, 23 août 1948.

Section 2

Une institution publique clé pour la protection des données : l'Autorité de protection des données

L'Autorité de protection des données[86] est l'autorité de contrôle belge en matière de traitements de données à caractère personnel. Le R.G.P.D., comme d'ailleurs la directive 95/46 avant lui, érige l'autorité de contrôle en « élément essentiel de la protection des données »[87]. Et pour cause. Le régime juridique de la protection des données risquerait bien de n'être qu'un vœu pieux sans une autorité chargée de faire connaître ces règles et de veiller à leur application dans la pratique[88].

L'A.P.D. est l'institution qui a succédé à la Commission de la protection de la vie privée[89]. Cette dernière était instituée depuis 1992. Elle jouait déjà un rôle de chien de garde pour protéger la vie privée des citoyens à l'occasion des traitements de leurs données par les entreprises et les pouvoirs publics. Malheureusement, le législateur n'avait pas jugé utile de lui donner de réels pouvoirs de sanction, et en particulier, le pouvoir d'imposer une amende. La C.P.V.P. ne faisait donc pas fort peur aux responsables de traitements, à l'image d'un chien de garde sans dent[90].

À l'occasion de l'adoption du R.G.P.D., le législateur belge n'a plus eu le choix. Il a été contraint de clarifier le statut et de renforcer les compétences de notre autorité de contrôle nationale. La C.P.V.P. a alors été rebaptisée « Autorité de protection des données », et encadrée par une nouvelle loi qui lui est consacrée à part entière, la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données »[91].

Les lignes qui suivent étudient la composition, le statut et les compétences de l'A.P.D.

A. La composition de l'A.P.D.

La composition de l'A.P.D. a été profondément modifiée par rapport à la composition de la C.P.V.P. jadis.

86 Ci-après, « A.P.D. ».

87 Cons. 62 de la directive 95/46 ; cons. 117 R.G.P.D.

88 Sur la raison d'être de l'autorité de contrôle, voy. É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, nos 63 et s. et C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base*, *op. cit.*, pp. 138 et s.

89 Ci-après, « C.P.V.P. ».

90 À ce sujet, voy. É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, nos 487 et s.

91 Ci-après, « loi A.P.D. ». Cette loi importante a été adoptée dans une urgence non nécessaire et souffre dès lors de lacunes regrettables. À ce sujet, voy. C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base*, *op. cit.*, pp. 137 et s.

Elle est désormais définie par les articles 7 et suivants de la loi A.P.D., que nous avons concrétisés par un schéma pour aider le lecteur dans la compréhension de ces dispositions assez fastidieuses.

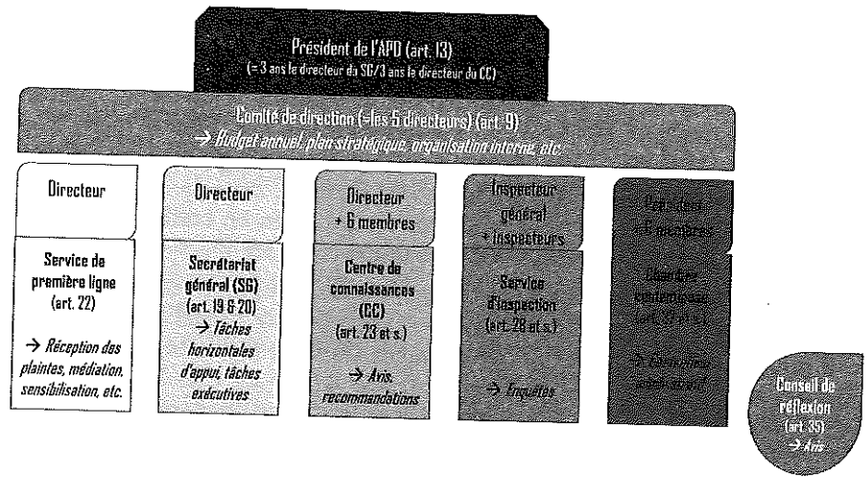


Schéma de la composition de l'A.P.D.

L'A.P.D. est composée de six organes, dont le comité de direction composé des directeurs des cinq autres organes.

Chacun de ces organes est dédié à l'exécution de missions dont il sera question ci-dessous.

À noter que le conseil de réflexion est indépendant de l'Autorité de protection des données. Il « représente la société dans son ensemble »[92] et « épaule [l'A.P.D.] dans ses orientations »[93]. L'idée est de permettre à l'A.P.D. de recueillir des avis « à caractère pluridisciplinaire »[94].

B. La compétence matérielle[95] de l'A.P.D.

L'A.P.D. est un contrôleur, un corégulateur et un conseiller[96].

92 Projet de loi portant création de l'Autorité de protection des données, préc., no 54-2648/001, p. 16.

93 *Ibid.*, p. 1.

94 *Ibid.*, p. 17.

95 Sur la compétence territoriale de l'A.P.D., voy. C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique. Manuel de base*, *op. cit.*, pp. 146 et s.

96 Dans le même sens, à propos de l'autorité de contrôle en général, voy. V. Verbruggen, « Titre 1. R.GPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR)*, *op. cit.*, p. 55.

1. L'A.P.D. contrôleur

Tout d'abord, l'A.P.D. est un contrôleur, chargé de veiller au respect effectif de la protection des données. À cet égard, les pouvoirs de l'A.P.D. ont été renforcés par rapport à ceux de la C.P.V.P.

L'A.P.D. dispose de *moyens juridiques classiques*. Par exemple, le service d'inspection est habilité à mener des enquêtes pour instruire le dossier, durant lesquelles il peut notamment « procéder à des examens sur place »[97], « saisir ou mettre sous scellés des biens ou des systèmes informatiques »[98], la chambre contentieuse peut « transmettre le dossier au parquet de Bruxelles »[99], l'« autorité de contrôle compétente »[100] peut introduire une action en cessation devant le président de première instance, siégeant comme en référé[101]…

Mais la capacité de réaction et d'intervention est encore renforcée grâce à des *moyens d'action plus souples, plus rapides et dès lors mieux adaptés* que les moyens traditionnels au caractère technique et rapide du secteur du numérique. Cette particularité n'est sûrement pas sans lien avec le constat dressé par l'Agence européenne des droits fondamentaux (FRA) en 2014 : l'autorité de contrôle étant conçue comme une instance à laquelle toute personne peut s'adresser directement pour mettre en œuvre ses droits, « les autorités de protection des données se sont révélées être la voie à suivre la plus populaire – et bien souvent la seule voie pertinente – pour les personnes demandant réparation dans les cas de violations de la protection des données »[102].

Ainsi par exemple, le service d'inspection peut ordonner le « gel temporaire du traitement de données » qui fait l'objet d'une enquête[103]. La chambre contentieuse peut, notamment, « formuler des avertissements et des réprimandes »[104], « ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données »[105].

La chambre contentieuse peut aussi « décider au cas par cas de publier ses décisions sur le site internet de l'Autorité de protection des données »[106]. La publicité entourant les décisions de l'A.P.D. présente plusieurs avantages. Grâce à cette transparence, la chambre prend pleinement conscience des problèmes en matière de protection des données et de leur origine. Lorsqu'il s'agit de

97 Art. 66, § 1er, 4°, de la loi A.P.D.
98 Art. 66, § 1er, 7°, de la loi A.P.D.
99 Art. 95, § 1er, 7°, de la loi A.P.D.
100 Art. 211, § 3, 2°, de la loi-cadre.
101 Art. 209 de la loi-cadre.
102 Agence européenne des droits fondamentaux (FRA), « Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE », 2014, p. 5, https://fra.europa.eu/fr/publication/2014/acces-aux-voies-de-recours-en-matire-de-protection-des-donnes-caractre-personnel.
103 Art. 70, al. 1er, de la loi A.P.D.
104 Art. 100, § 1er, 5°, de la loi A.P.D.
105 Art. 100, § 1er, 10°, de la loi A.P.D.
106 Art. 95, § 1, 8°, de la loi A.P.D.

problèmes ayant lieu dans une administration, le ministre de tutelle peut être interpellé. En outre, et particulièrement s'agissant du secteur privé, la dénonciation publique des illégalités commises en matière de protection des données est une sanction redoutable en ce qu'elle porte atteinte à la réputation de l'entreprise ou de l'institution qui en est l'auteure. Ce type de sanction peut s'avérer plus efficace qu'une amende. Les décisions de la chambre contentieuse qui font l'objet d'une publication sont accessibles sur le site internet de l'A.P.D.[107].

Dès lors, compte tenu du fait que ce type de publication a un impact bien plus conséquent qu'une simple formalité administrative, il est dommage que le législateur n'ait pas précisé les critères en fonction desquels l'A.P.D. doit les publier, ou non.

La chambre contentieuse peut également « donner des amendes administratives »[108]. Par exemple, entre avril 2019 et décembre 2019, l'A.P.D. a déjà imposé une amende à quatre candidats aux élections qui ont violé la protection des données en utilisant, à des fins électorales, des données collectées à de toutes autres fins[109].

Le pouvoir d'amende fait grand bruit. En effet, la C.P.V.P. ne disposait pas de ce pouvoir, car, même si la directive 95/46 permettait aux États membres d'octroyer ce pouvoir aux autorités de contrôle nationales, le législateur n'a pas estimé utile de le faire. Depuis, le R.G.P.D. impose aux États européens de doter leur(s) autorité(s) de contrôle de cette prérogative. Dès lors, l'A.P.D. a le pouvoir d'imposer cette sanction dans les cas qui le nécessitent, en veillant à ce qu'elle soit effective, proportionnée et dissuasive. L'amende peut d'ailleurs constituer la seule sanction imposée au responsable du traitement ou intervenir en complément d'une autre sanction.

Quant au montant de l'amende, celle-ci peut atteindre des plafonds très importants, pouvant aller jusqu'à 20.000.000 euros ou 4 % du chiffre d'affaires annuel mondial d'une entreprise. Ces montants s'expliquent par le souci de faire peur aux grandes entreprises qui traitent massivement des données à caractère personnel, notamment les « GAFAM »[110].

Une administration peut-elle se voir infliger une amende ? En principe, non. À la fin de son considérant 144, le R.G.P.D. affirme la possibilité, pour les États membres, de décider que leurs autorités publiques ne peuvent pas faire l'objet d'amendes administratives, sans autre explication. Le législateur fédéral belge s'est saisi de cette possibilité. La loi du 30 juillet 2018 affirme, en son

107 www.autoriteprotectiondonnees.be/decisions.
108 Art. 100, § 1er, 13°, de la loi A.P.D.
109 www.rtbf.be/info/regions/liege/detail_protection-des-donnees-reprimande-et-5000-euros-d-amende-pour-le-bourgmestre-de-pepinster?id=10379153 ; www.autoriteprotectiondonnees.be/news/lautorite-de-protection-des-donnees-prononce-une-sanction-dans-le-cadre-dune-campagne ; É. Degrave, « L'autorité de protection des données, un chien de garde de la vie privée des citoyens », www.justice-en-ligne.be, à paraître.
110 Google, Apple, Facebook, Amazon et Microsoft.

article 221, § 2, que l'article 83 du R.G.P.D. «ne s'applique pas aux autorités publiques et à leurs préposés ou mandataires».

Précisons d'ailleurs que le législateur fédéral a décidé que le terme «autorité publique» visait non seulement l'État fédéral, mais également «les entités fédérées et les autorités locales»[111], raison pour laquelle l'article 221 de la loi s'applique également aux Communautés, aux Régions et aux pouvoirs locaux...

L'article 221, § 2, prévoit toutefois une exception pour les «personnes morales de droit public qui offrent des biens ou des services sur un marché». Celles-ci restent passibles d'une amende[112]. La loi ne définit pas le terme «marché» mais les travaux préparatoires de cette loi révèlent que l'on vise le marché des transports, de la livraison de colis, de la téléphonie, etc.[113]. L'idée est de ne pas créer de discrimination entre ces entreprises publiques (telles que Proximus) et les entreprises privées (telles que VOO).

L'exemption d'amende pour les autorités publiques pose question. N'y a-t-il pas là une discrimination par rapport au secteur privé?

La section de législation du Conseil d'État[114] et la Commission de la protection de la vie privée[115] répondent par l'affirmative. Entre autres arguments, la discrimination possible est liée au fait que les institutions du secteur public et du secteur privé peuvent être amenées à traiter les mêmes données. Tel est le cas, par exemple, des données d'identification (nom, prénom, date de naissance...), des données fiscales, traitées par le S.P.F. Finances, mais aussi les banques notamment, des données de santé traitées par les institutions de sécurité sociale, mais aussi les assurances, notamment. Or, l'exclusion totale d'amende pour les autorités publiques prive l'A.P.D. d'un pouvoir de sanction qui a un effet dissuasif. Cette absence de sanction dissuasive n'est pas compensée par ailleurs. Certes, des sanctions pénales peuvent être imposées. Mais les montants sont moins dissuasifs et dans bien des cas, en vertu de l'article 7*bis* du Code pénal, la personne morale de droit public ne peut faire l'objet que d'une simple déclaration de culpabilité[116]. Pour cette raison, il a notamment été suggéré au législateur de maintenir la possibilité de sanctionner une autorité publique d'une amende, tout en organisant des montants d'amende moins élevés. Cela n'aurait évidemment aucun sens d'imposer une amende de 20.000.000 euros à une commune...

Néanmoins, le législateur n'a pas suivi ces recommandations si bien que cette exemption totale d'amende pour les autorités publiques fait actuellement l'objet d'un recours en annulation devant la Cour constitutionnelle.

111 Art. 5, 1°, de la loi-cadre.

112 Art. 221, § 2, *in fine* de la loi-cadre.

113 Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/002, p. 55.

114 S.L.C.E., avis n° 63.192/2 du 19 avril 2018 sur un avant-projet de loi «relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel», *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, pp. 450 et s.

115 C.P.V.P., avis n° 33/2018 du 11 avril 2018 sur un avant-projet de loi «relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel», *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, pp. 846 et s.

116 Voy. L. Gérard, «Sanctions», *in* É. Degrave (dir.), *L'ABC du RGPD. Dictionnaire pratique à destination des administrations*, *op. cit.*, pp. 57 et 58.

2. L'A.P.D. corégulateur

En tant que corégulateur, l'autorité de contrôle est un relais utile du législateur au niveau de la définition des règles de protection des données et de leur mise en œuvre.

À cet égard, il revient, par exemple, au secrétariat général de l'A.P.D. d'«établir la liste des traitements qui requièrent une analyse d'impact relative à la protection des données»[117], ce qui est d'ailleurs chose faite[118].

Autre exemple, le secrétariat général doit «promouvoir l'introduction de mécanismes de certifications et approuver les critères de certification»[119]. À cet égard, il se fie notamment aux lignes directrices fixées récemment par le Comité européen de protection des données dans le but d'harmonisation les pratiques au sein de l'Union européenne[120].

3. L'A.P.D. conseiller

L'A.P.D. est un conseiller pour les *responsables du traitement*, les *personnes concernées*, le *public en général*.

Ainsi, le service de première ligne promeut «la protection des données auprès du public, en accordant une attention spécifique aux mineurs»[121], elle promeut aussi «auprès des responsables de traitement et des sous-traitants la prise de conscience de leurs obligations»[122].

Ce service est également chargé de fournir des «informations relatives à l'exercice de leurs droits aux personnes concernées»[123]. On espère que le service de première ligne sera particulièrement attentif à cet aspect de ses missions. Il importe de pouvoir guider utilement les personnes concernées dans les méandres de l'univers numérique, de les aider à faire valoir leurs droits auprès des responsables de traitement, qu'il s'agisse d'administrations ou d'entreprises.

117 Art. 20, § 1, 2°, de la loi A.P.D.

118 Voy. www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste_des_traitements_AIPD.pdf.

119 Art. 20, § 1er, 5°, de la loi A.P.D. et www.autoriteprotectiondonnees.be/codes-de-conduite.

120 www.dataprotectionauthority.be/sites/privacycommission/files/documents/EDPB_Guidelines_4_2018_accreditation_en.pdf.

121 Art. 22, § 1er, 3°, de la loi A.P.D.

122 Art. 22, § 1er, 4°, de la loi A.P.D.

123 Art. 22, § 1er, 5°, de la loi A.P.D.

À cet égard, il serait très utile que le service de première ligne complète, en profondeur, la rubrique «les différents droits» présentée sur le site internet de l'Autorité de protection des données. Il faudrait par exemple mettre à disposition des citoyens un «courrier type» pour l'exercice du droit d'accès aux données, comme il en existait un jadis sur le site internet de la C.P.V.P. Il serait judicieux également de présenter de manière claire et compréhensible les outils qui existent déjà, en ligne, pour contrôler l'usage qui est fait de nos données, par les administrations notamment[124]. En effet, jusqu'ici, les règles de protections des données ont manqué d'effectivité, car elles étaient peu connues et peu appliquées en pratique. Aujourd'hui, il est primordial que les citoyens, qui ont des droits, les exercent. C'est le rôle de l'A.P.D. en général, et du service de première ligne en particulier, de les y aider.

Par ailleurs, l'A.P.D. est aussi un conseiller pour *les législateurs et les gouvernements,* par l'intermédiaire du Centre de connaissances[125].

C. Le statut de l'A.P.D.

Au niveau de son statut, l'A.P.D. est aujourd'hui une autorité administrative indépendante conçue selon le modèle des autres autorités de régulation que sont la CREG (dans le secteur de l'énergie) et l'I.B.P.T. (dans le secteur des télécommunications).

L'objectif est double : d'une part, il s'agit de consolider l'indépendance de l'A.P.D. (1) et, d'autre part, de renforcer sa responsabilité (2).

1. L'indépendance de l'A.P.D.

Une caractéristique majeure de l'autorité de contrôle est son indépendance. Une autorité de contrôle forte et efficace doit être indépendante des responsables de traitement qu'elle contrôle, qu'ils soient publics ou privés. C'est pourquoi le R.G.P.D. consacre une section entière au «statut d'indépendance» de l'autorité de contrôle, affirmant notamment que «chaque autorité de contrôle exerce en toute indépendance les missions et les pouvoirs dont elle est investie, conformément au présent règlement»[126].

Si cette exigence était déjà présente dans la directive 95/46, elle est substantiellement affinée dans le R.G.P.D., qui intègre[127] la jurisprudence de la

124 On songe, par exemple, à l'outil «Mon dossier» sur le site internet du Registre national, évoqué à l'entame de cette étude.

125 Art. 23, § 1er, de la loi A.P.D. Quant à la question de savoir si l'A.P.D. doit obligatoirement être consultée pour tout texte en projet qui a trait à un traitement de données à caractère à caractère personnel, voy. C. DE TERWANGNE et É. DEGRAVE, *La protection des données à caractère personnel en Belgique. Manuel de base*, *op. cit.*, pp. 147 et s.

126 Art. 52.1 R.G.P.D.

127 Voy. art. 52 R.G.P.D.

Cour de justice de l'Union européenne[128] relative à l'indépendance de l'autorité de contrôle[129].

L'indépendance de l'A.P.D. est *institutionnelle*. Cela signifie qu'elle doit agir en «toute» indépendance, selon l'article 52.1 du R.G.P.D., c'est-à-dire sans influence extérieure. Cela exclut, par exemple, un contrôle de tutelle de l'État sur l'autorité de contrôle[130].

L'indépendance de l'A.P.D. est également *organisationnelle et budgétaire*. En effet, selon le R.G.P.D., l'autorité de contrôle doit disposer des «ressources humaines, techniques et financières, ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs [...]»[131]. Elle doit également disposer «d'un budget annuel public propre, qui peut faire partie du budget global national ou d'une entité fédérée»[132]. À cet égard, on regrette que la mise en place de l'A.P.D. ait dû se faire de manière «budgétairement neutre»[133] alors que l'entrée en application du R.G.P.D. a offert une grande publicité à la matière, qui s'est accompagnée notamment d'une augmentation du nombre de plaintes introduites auprès de l'A.P.D.[134].

Enfin, l'indépendance de l'A.P.D. est aussi celle de ses *membres*. Dans l'exercice de leur mission, ils doivent être «libres de toute influence extérieure»[135], s'abstenir de tout acte ou activité professionnelle incompatible avec leurs fonctions[136]. Ces éléments se retrouvent dans les articles 43 et 44 de la loi A.P.D., qui précisent notamment qu'une activité incompatible est «une activité pouvant bénéficier directement ou indirectement des décisions et prises de position que peut prendre l'Autorité de protection des données»[137].

2. La responsabilité de l'A.P.D.

L'A.P.D. est désormais dotée de la personnalité juridique. Cela signifie que l'A.P.D. voit sa responsabilité renforcée puisqu'elle pourrait être elle-même assignée en justice et condamnée si, par exemple, une abstention fautive d'agir devait lui être reprochée.

128 Ci-après, «C.J.U.E.».

129 Au sujet de cette jurisprudence, voy. É. DEGRAVE, «Titre 11. L'autorité de contrôle», *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR)*, coll. CRIDS, Bruxelles, Larcier, 2018, pp. 599 à 601.

130 C.J.U.E. (Gde ch.), 9 novembre 2010, préc., § 58.

131 Art. 52.4. R.G.P.D.

132 Art. 52.6. R.G.P.D.

133 Projet de loi portant création de l'Autorité de protection des données, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-2640/006, p. 15.

134 Entretien avec un membre de l'A.P.D. en mars 2019.

135 Art. 52.2 R.G.P.D.

136 Art. 52.3 R.G.P.D.

137 Art. 44, § 1er, de la loi A.P.D.

Par ailleurs, la responsabilité de l'A.P.D. est également renforcée du fait que les décisions qu'elle prend sont susceptibles de recours et, donc, d'un contrôle juridictionnel. En effet, l'article 78 du R.G.P.D. consacre le droit à un recours juridictionnel et effectif contre les décisions juridiquement contraignantes adoptées par une autorité de contrôle.

a) Les recours contre les décisions de la chambre contentieuse

En vertu de l'article 108, § 2, de la loi-cadre, « un recours peut être introduit contre les décisions de la chambre contentieuse [...] devant la Cour des marchés qui traite l'affaire selon les formes du référé ». Par exemple, une entreprise se voyant imposer une amende pour avoir violé les règles de protection des données pourra contester cette sanction devant la Cour des marchés, dans le cadre d'une procédure qui prend les formes du référé mais aboutit à une décision au fond.

À notre sens, il est regrettable que le législateur ait organisé ce recours devant la Cour des marchés. Il s'agit d'une cour composée de juges spécialisés en matière financière. Comme nous l'avons affirmé en Commission de la justice lors des discussions préparatoires à l'adoption de la loi A.P.D., « la protection des données est un des moyens visant à protéger les droits fondamentaux des citoyens. Le but n'est pas de stimuler une concurrence économique entre entreprises. Le juge naturel, si on parle d'une autorité administrative indépendante, n'est-il pas le Conseil d'État ? »[138]. On craint que les litiges concernant la violation de la vie privée et de la protection des données à caractère personnel des citoyens se réduisent en réalité à des enjeux de concurrence entre entreprises, la donnée n'étant plus qu'un enjeu exclusivement financier. Le fait qu'un droit fondamental soit en jeu ne recevra pas nécessairement toute l'attention nécessaire.

b) Les recours contre les décisions des autres organes de l'A.P.D.

Les sanctions imposées par la chambre consciencieuse ne sont pas les seules décisions contraignantes que peut prendre l'A.P.D. Ainsi qu'on l'a dit[139], l'A.P.D., via son secrétariat général, peut décider de refuser d'approuver un code de conduite. Via son service d'inspection, elle peut décider d'ordonner l'effacement de données. Via son service de première ligne, elle peut décider de déclarer irrecevable une plainte ou une requête, etc. Ce sont des décisions juridiquement contraignantes qui doivent pouvoir faire l'objet d'un recours juridictionnel également. D'ailleurs, l'article 4, § 3, de la loi A.P.D. affirme que « toute décision juridiquement contraignante de l'Autorité de protection des

138 Projet de loi portant création de l'Autorité de protection des données, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-2648/006, p. 50.

139 Voy. *supra*.

données [...] fait référence aux recours qui peuvent être introduits contre la décision ».

Or, la loi A.P.D. est muette quant aux recours qui peuvent être introduits contre les décisions juridiquement contraignantes qui émanent d'autres organes que la chambre contentieuse. À notre sens, l'A.P.D. peut être qualifiée d'autorité administrative[140]. Partant de là, les décisions de l'A.P.D. qui ne sont pas rendues par la chambre contentieuse doivent pouvoir faire l'objet d'un recours en annulation devant le Conseil d'État, en vertu de l'article 14, § 1er, 1°, des lois coordonnées sur le Conseil d'État, tout comme d'ailleurs les décisions de la CREG par exemple.

140 Pour plus de détails, voy. C. DE TERWANGNE et É. DEGRAVE, *La protection des données à caractère personnel en Belgique. Manuel de base, op. cit.*, pp. 153 et s.