L'administration belge organisée en réseaux

Degrave, Élise

Published in:
Données urbaines et smart cities

Publication date:
2017

Document Version
le PDF de l'éditeur

ÉTUDE DE CAS

L'administration belge organisée en réseaux : réutilisation des données à caractère personnel et protection de la vie privée

Élise Degrave
Chargée de cours à la faculté de droit de l'université de Namur
et codirectrice de la chaire e-Gouvernement de l'université
de Namur, Belgique

À l'heure des *smart cities*, l'administration en ligne reçoit une attention particulière. Aujourd'hui, un billet d'avion pour faire le tour du monde s'achète en quelques clics depuis son Smartphone et à n'importe quel moment, alors que l'obtention d'un document administratif suppose encore bien souvent que l'on se déplace à l'administration en se soumettant à des horaires contraignants et en fournissant moult documents. Le développement de l'administration en ligne permet progressivement d'atténuer des agacements de ce genre.

Depuis plusieurs années, la Belgique attache une attention particulière à la réutilisation des données à caractère personnel des citoyens dans le secteur public. L'idée est de mettre en place des outils de traitements de ces données pour augmenter l'efficacité de l'administration tout en protégeant la vie privée des citoyens concernés.

Aujourd'hui, ces réflexions ont abouti à la mise en place d'un modèle d'administration tout à fait inédit, structuré en réseaux. Il en résulte un

bouleversement dans la structure de l'administration mais aussi dans son mode de fonctionnement[1].

I – L'objectif de la collecte unique des données

L'organisation de l'administration a été pensée par rapport à un objectif clair, celui de la collecte unique des données.

Avant le développement de l'e-Gouvernement, l'administration était structurée « en silos[2] », ce qui signifie qu'elle était composée de ministères distincts et cloisonnés. Chacun gérait ses propres données, les échanges de celles-ci entre ces ministères étaient donc rares. Ainsi, lors des débats parlementaires relatifs au projet de loi relative à l'informatique, aux fichiers et aux libertés en France, a-t-on mis en évidence « le cloisonnement des administrations et le peu de goût que celles-ci ont à l'ordinaire pour se communiquer les données qu'elles détiennent comme des trésors précieux. L'informatique, par le moyen des interconnexions, rend fluide et automatique la circulation des informations[3] ». Le même constat pouvait être fait en Belgique.

Le développement de l'e-Gouvernement rompt radicalement avec ce type de structure administrative. Il est guidé par un objectif à atteindre, la collecte unique des données, qui est rendue possible grâce à l'informatique. Ce principe consiste à ne demander qu'une seule fois aux citoyens les informations qui les concernent, à la différence de ce qui se faisait auparavant dans l'administration, lorsque les individus devaient souvent communiquer leurs données à chaque administration avec laquelle ils étaient en contact. En d'autres termes, dès que le citoyen a communiqué une information d'un certain type à une administration, les autres administrations ne peuvent plus la lui réclamer à nouveau.

1. Cette contribution est inspirée des textes suivants de la même auteure : *e-Gouvernement et protection de la vie privée. Légalité, transparence et contrôle*, Larcier, coll. « Crids », Bruxelles, 2014 ; « L'intégrateur de service fédéral au cœur de la simplification administrative », *Adm. publ.*, 2014, p. 518-536 ; « Transparence administrative et traitements de données à caractère personnel », note d'observation sous Cass. (1re ch.), 14 janv. 2013, *Revue du droit des technologies de l'information*, 2014, p. 518-536.
2. Bundshuch-Rieseneder F., *"Governance and E-Governance in the Frame of Bologna Process"*, *in* Come T. et Rouet G., *Bologna Process, European Construction, European Neighbourhood Policy*, 2011, Bruxelles, Bruylant, p. 253 et 254 – Maisl H., « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », *in* Chatillon G. et du Marais B. (dir.), *L'administration électronique au service des citoyens*, 2003, Bruxelles, Bruylant, p. 349 à 359 – Duaso Calès R., *Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau*, thèse, sept. 2015, université de Montréal et université Panthéon-Assas Paris II, sept. 2011, p. 37 à 44.
3. Assemblée nationale (France), Première session ordinaire de 1977-1978, Compte-rendu intégral 2e séance, 4 oct. 1977, « Débats relatifs au projet de loi Informatique et libertés », p. 5782.

La collecte unique doit être soutenue par la réutilisation des données à caractère personnel 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, tout en respectant le principe de la collecte unique des données.

II – Le modèle de l'administration en réseaux

Pour mettre en œuvre efficacement l'échange des informations entre administrations, la Belgique s'engage, depuis plusieurs années, dans un modèle de circulation des données à caractère personnel tout à fait 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.

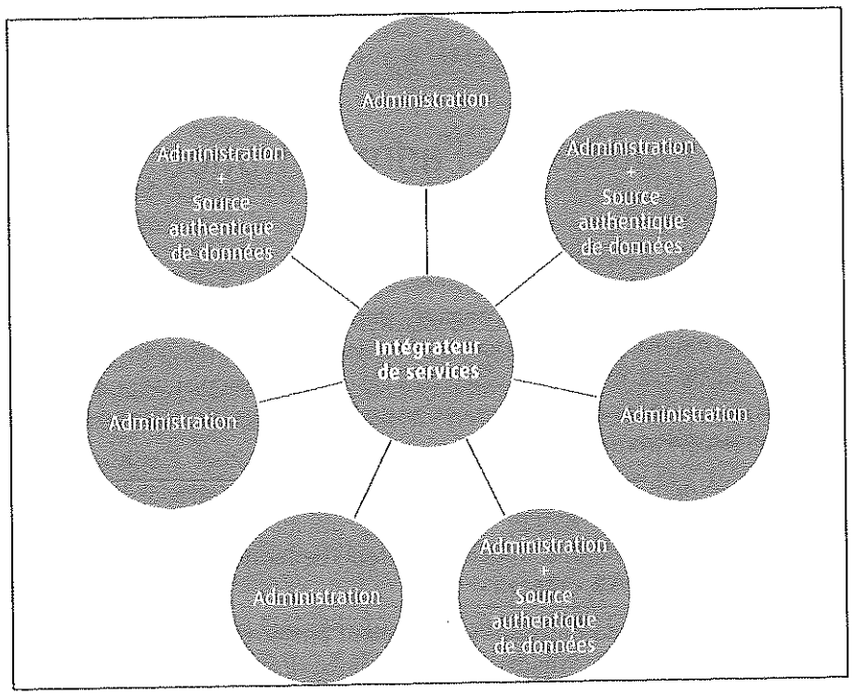
Plus précisément, dans un premier temps, les administrations ayant un point commun (par exemple, un objet de travail commun ou l'appartenance à une même entité, fédérale ou fédérée) sont regroupées au sein d'un ensemble appelé « réseau ».

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, qui sont 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 « plateforme 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, d'ores et déjà, schématiser comme suit le modèle d'un réseau d'administrations comprenant un intégrateur de services.

Figure 1 : 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

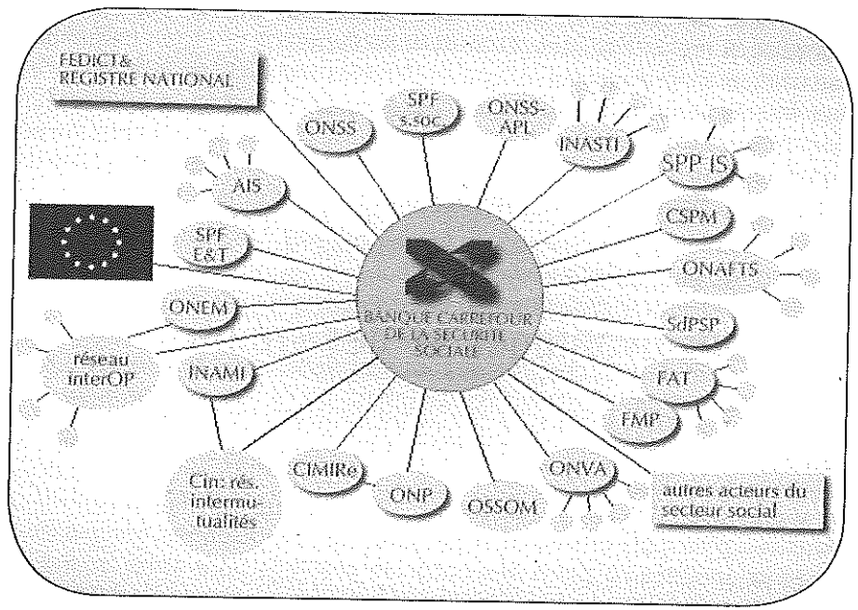


Depuis quelques années, plusieurs réseaux d'administrations ont progressivement été créés au sein du secteur public belge. Ils comprennent chacun, en leur cœur, un intégrateur de services.

Les premiers réseaux créés sont des réseaux dits « sectoriels », car ils sont liés à un domaine particulier de l'administration. L'intégrateur de services placé au cœur de ces réseaux sectoriels est qualifié d'intégrateur « vertical » par opposition aux intégrateurs de services « horizontaux » décrits ci-après. 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[4]. S'en est suivi la création, en 2008, du réseau sectoriel de la santé, au sein duquel la plateforme eHealth assume le rôle d'intégrateur de services[5].

4. L., 15 janv. 1990, relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité sociale, *MB*, 22 févr. 1990. Ci-après L., 15 janv. 1990, relative à la Banque-carrefour de la Sécurité sociale.
5. L., 21 août 2008, relative à l'institution et à l'organisation de la plateformeeHealth et portant diverses dispositions, *MB*, 13 oct. 2008.

Figure 2 : Exemple d'intégrateur de services vertical : la Banque-carrefour de la Sécurité sociale placée au cœur du réseau de la Sécurité sociale



Bien que ce modèle soit séduisant, la multiplication d'intégrateurs de services verticaux présente une difficulté particulière, à savoir que les administrations qui ont besoin d'informations relatives à un citoyen dont elles gèrent le dossier sont contraintes de s'adresser à différents intégrateurs de services en fonction du type de donnée recherchée. Or, ces derniers ont chacun leurs outils spécifiques et leurs procédures particulières.

Dès lors, dans un deuxième temps et depuis peu, des réseaux et intégrateurs de services dits « horizontaux » ou encore « transversaux » sont mis en place. Ces réseaux regroupent des administrations en fonction de leur appartenance à l'entité fédérale ou à une entité fédérée. Ils comprennent un intégrateur de services chargé d'assurer la circulation des données entre les administrations concernées. Ainsi, en 2012, est créé l'intégrateur de services fédéral. Au niveau des entités fédérées, l'intégrateur de services flamand est créé en 2012 pour assurer l'échange électronique des données au sein du réseau flamand constitué des institutions de la Communauté flamande et de la région flamande[6]. Il s'agit du *Coördinatiecel Vlaams e-Government* (*CORVE*). Les administrations de la Communauté française et de la région wallonne sont également regroupées au sein d'un réseau

6. D., 13 juill. 2012, portant création et organisation d'un intégrateur de services flamand, *MB*, 1er août 2012.

au sein duquel œuvre, depuis 2013[7], un intégrateur de services dénommé « Banque-carrefour d'échanges de données » (BCED). Grâce à ces intégrateurs horizontaux, les administrations peuvent s'adresser à l'intégrateur de services de l'entité dont elles font partie (État fédéral, Communauté française et région wallonne, Communauté flamande et région flamande), sans devoir s'interroger sur le type de données recherchées pour identifier leur interlocuteur. L'intégrateur se charge ensuite d'acheminer l'information recherchée vers l'administration qui l'a demandée, au besoin en contactant lui-même les intégrateurs de services verticaux que sont la Banque-carrefour de la Sécurité sociale et la plateforme eHealth.

III – Des avantages et des craintes

De toute évidence, l'efficacité de l'administration est renforcée grâce à l'échange rapide d'informations exactes et à jour. En outre, puisque ces données sont disponibles sous forme électronique, on peut les réutiliser et y appliquer différents traitements. C'est ce que l'on fait notamment pour contrôler plus efficacement les citoyens. Par exemple, progressivement se mettent en place des outils de profilage pour lutter contre la fraude fiscale et sociale. Il s'agit de regrouper des données très différentes au sein d'une grande base de données appelée « entrepôt de données » ou « *data warehouse* » et d'y appliquer des calculs très puissants appelés « algorithmes de fraude », basés notamment sur des calculs statistiques. Ce faisant, l'ordinateur peut identifier des personnes suspectées de fraude. Ces outils semblent très efficaces puisque, selon les dires d'inspecteurs sociaux, jusqu'à présent, la plupart des personnes suspectées de fraude se sont révélées, après contrôle, être effectivement coupables[8].

Le citoyen voit également ses tâches facilitées. Il peut accéder à nombre d'informations en ligne et effectuer des transactions administratives à tout moment depuis son ordinateur. Il lui est également épargné certaines démarches administratives grâce à l'automatisation des procédures. À cet égard, par exemple, une application informatique créée par

7. D., 4 juill. 2013, portant assentiment de l'accord de coopération entre la région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *MB*, 23 juill. 2013.

8. Pour de plus amples précisions sur la technique du profilage : Recommandation CM/Rec(2010)13 du Comité des ministres du Conseil de l'Europe aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, disponible sur le site *www.coe.int* – Hildebrandt M., *"Who is Profiling Who ? Invisible Visibility"*, *in* Gutwirth S., Poullet Y., De Hert P., de Terwangne C. et Nouwt S.(dir.), *Reinventing Data Protection ?*, Dordrecht, Springer, 2009, p. 241 – Papakonstantinou V., *"A Data Protection Approach to Data Matching Operations Among Public Bodies"*, *International journal of Law and Information Technology* 2001, vol. 9, n° 1, p. 62-63 – Dinant J.-M., Lazaro C., Poullet Y., Lefever N. et Rouvroy A., « L'application de la Convention 108 au mécanisme de profilage. Éléments de réflexion destinés au travail futur du Comité consultatif », *T-PD*, 01, mars 2008, p. 5 – Degrave É., *L'e-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, n°s 40 et s.

l'intégrateur de services fédéral et dénommée eBirth facilite l'échange des données relatives à la naissance d'un enfant. Ce service part du constat que tant les communes que la Communauté française et le SPF Économie ont besoin d'informations relatives à chaque naissance. Jadis, ces administrations obtenaient ces informations *via* des formulaires papier envoyés par les hôpitaux. Aujourd'hui, les hôpitaux se connectent au portail eBirth, encodent les données requises, et celles-ci sont acheminées respectivement vers les communes, la Communauté française et le SPF Économie[9].

De toute évidence, l'e-Gouvernement est donc séduisant. Mais certaines craintes surgissent. En général, lorsqu'on évoque le danger d'utiliser les technologies dans l'administration, on songe au spectre de *Big Brother*. C'est l'idée d'un État omniscient, qui saurait tout de tout le monde et pourrait surveiller chaque individu. Cette crainte est justifiée. Mais il existe également un autre danger tout aussi fondamental, plus rarement mis en évidence : celui de créer progressivement une administration kafkaïenne[10], c'est-à-dire une administration à ce point technique et complexe, à ce point distante, qu'elle en deviendrait incompréhensible et dès lors incontrôlable.

Face à ce constat, il faut veiller à ce que, dans l'e-Gouvernement, le citoyen ne soit pas exclu de cette évolution technologique et qu'il puisse continuer à comprendre et contrôler l'action de l'administration. Pour ce faire, certains moyens de contrôle de l'administration en réseaux paraissent intéressants.

IV – Le contrôle de l'administration en réseaux

A – La transparence des données

La collecte unique des données facilite la tâche des administrations et des citoyens mais risque de provoquer un sérieux dysfonctionnement administratif si les sources authentiques de données contiennent des données incorrectes. En effet, ainsi qu'on l'a dit, la mise en œuvre de la collecte unique des données est fondée sur une réutilisation maximale des données issues des

9. Pour plus d'informations sur eBirth : la présentation générale d'eBirth disponible à l'adresse *www.ehealth.fgov.be/fr/services-en-ligne/ebirth/presentation-d-ebirth*

10. Solove D., *"I've Got Nothing to Hide' and Other Misunderstandings of Privacy"*, *San Diego Law Review* 2007, vol. 44, 745, p. 745-772.

sources authentiques. Si une donnée est erronée, un « effet domino[11] » se produit puisque l'erreur est démultipliée autant de fois que la donnée est réutilisée. Le travail de l'ensemble des administrations ayant utilisé la donnée échangée en pâtit alors. Il pourrait donc arriver qu'un citoyen soit soumis à une décision administrative fondée sur une donnée erronée. Dans cette hypothèse, on peut raisonnablement penser que, étonné face à pareille décision, il veuille comprendre d'où vient l'erreur. Contactant l'administration ayant pris cette décision, celle-ci pourrait lui répondre que les informations sur la base desquelles a été prise ladite décision administrative lui ont été fournies par l'intégrateur de services et qu'elle n'en connaît pas l'origine. Face à pareille situation, comment le citoyen peut-il savoir où se trouvent ses données et obtenir que les erreurs les affectant éventuellement soient corrigées ?

Par ailleurs, chaque citoyen est contraint de donner à l'administration un grand nombre d'informations relatives à de nombreux aspects de leur vie personnelle : coordonnées, composition du ménage, numéro de téléphone, situation financière, caractéristiques médicales justifiant l'octroi d'une allocation pour personne handicapée, etc. Ces informations étant aujourd'hui enregistrées électroniquement dans des bases de données, elles sont aisément et rapidement accessibles. Il peut donc être tentant, pour un agent de l'administration, de céder à la curiosité et d'aller consulter des informations auxquelles il a accès depuis son ordinateur. On pense, par exemple, à la consultation du registre DIV par des policiers ayant repéré, sur la route, de jolies conductrices à qui ils désirent téléphoner, ou encore à la consultation du Registre national par un fonctionnaire communal dans le but de retrouver l'adresse de son ancienne compagne[12]. Il s'agit là d'utilisations abusives des bases de données de l'administration qui doivent être sanctionnées. Encore faut-il pouvoir établir qui a accédé illégalement à quelles informations.

Les droits d'accès aux données et de rectification des données erronées peuvent aider le citoyen à contrer les risques d'erreur et d'abus dans l'utilisation des données, comme l'expliquent les lignes qui suivent.

Conformément à l'article 10 de la loi du 8 décembre 1992 qui transpose l'article 12 de la directive 95/46/CE[13], chaque citoyen a le droit de connaître un bon nombre d'informations relatives à l'usage qui est fait de ses données[14]. Il peut donc s'adresser à chaque administration qui détient des

11. CPVP, avis n° 11/2009, 29 avr. 2009, concernant le projet d'arrêté du gouvernement flamand portant exécution du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, p. 3, n° 6.
12. À ce sujet : CE, 26 avr. 2005, *Van Merris*, n° 143683.
13. Parlement européen et Conseil, dir. 95/46/CE, 24 oct. 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JO*, n° L 281, 23 nov. 1995, p. 31-50.
14. L., 8 déc. 1992, art. 10 – A. royal, 13 févr. 2001, portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *MB*, 13 mars 2001 – E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, n°s 331 et s. Pour un cas d'application dans l'administration : Cass. 1re ch., 14 janv. 2013, *RDTI*, 2013, p. 53 et s, note E. Degrave « Transparence administrative et traitements de données caractère personnel ».

données à son sujet en demandant les données exactes qui figurent dans son dossier, les raisons pour lesquelles elles sont enregistrées, à qui elles ont déjà été transmises et/ou le seront ultérieurement, pendant combien de temps elles seront conservées, etc. S'il constate des erreurs dans ses données, il a le droit d'exiger qu'elles soient rectifiées. Néanmoins, la procédure actuelle d'accès et de rectification des données est fastidieuse[15].

À notre sens, une manière de simplifier l'exercice des droits d'accès et de rectification serait de développer un portail Internet sur lequel le citoyen devrait s'identifier à l'aide de sa carte d'identité électronique. Ensuite, il verrait apparaître un organigramme sur lequel figurerait l'ensemble des sources authentiques détenant des données à son sujet. En cliquant sur le nom des sources authentiques, les données exactes enregistrées s'afficheraient à l'écran. En cas d'erreurs affectant l'une ou l'autre donnée, le citoyen pourrait signaler l'erreur en cliquant sur un onglet « Rectification ». Par ailleurs, le portail Internet devrait également lui laisser la possibilité d'accéder à l'historique des consultations de ses données. Pour chaque source authentique, le citoyen pourrait ainsi connaître les services ou les personnes ayant accédé à ses données. Il faudrait également prévoir que le parcours des données s'affiche aussi à l'écran pour comprendre aisément quelle administration a transmis quelle donnée à l'intégrateur de services et dans quel but.

B – L'exemple du portail « Mon dossier » du Registre national

Dans cette perspective, le Registre national propose déjà un outil très intéressant.

Le citoyen peut accéder à un portail Internet appelé « Mon dossier » en se connectant sur le site *https://mondossier.rrn.fgov.be/* Il doit s'y identifier à l'aide de sa carte d'identité et d'un lecteur de carte.

En se connectant au portail « Mon dossier », la personne concernée accède à deux types d'informations : les données de contenu détenues par le Registre national, ainsi que les données de consultation.

Concernant la première, citoyen peut consulter les données enregistrées à son sujet dans la source authentique qu'est le Registre national, telles que ses nom, prénoms, date de naissance, adresse mais également la profession, des données relatives à son permis de conduire, à sa participation

15. Il faut envoyer à chaque administration une lettre signée et accompagnée d'une photocopie de la carte d'identité en indiquant clairement les informations que l'on recherche. L'administration dispose de quarante-cinq jours pour répondre à la demande, et éprouve souvent elle-même des difficultés pour formuler ses réponses. En outre, l'exercice de ces droits est particulièrement fastidieux dans le contexte de l'administration en réseau puisque l'enregistrement des données, étant éparpillé entre diverses sources authentiques du réseau, rend difficile de deviner quelle institution détient quelle donnée.

Elle dispose de moyens d'action intéressants dans le contexte de l'e-gouvernement. À l'image d'un médiateur, la CPVP reçoit les plaintes des citoyens lorsqu'elles touchent à la protection de la vie privée. Une médiation peut ensuite être organisée entre la personne concernée et l'institution visée. D'autres moyens d'action sont à sa disposition, tels que le droit d'intenter une action judiciaire dans l'intérêt collectif[22]. Les traitements de données illégaux commis dans l'administration peuvent ainsi être dénoncés en justice par l'autorité de protection des données.

Néanmoins, à certains égards, le contrôle exercé par la CPVP manque d'efficacité et d'effectivité. Par exemple, cette institution n'a encore jamais exercé l'action judiciaire dans l'intérêt collectif. Ce recours reste d'ailleurs assez méconnu. De plus, pour permettre à la CPVP d'agir plus efficacement, il serait judicieux d'augmenter ses moyens humains et de lui conférer plus de moyens d'action, tels qu'un pouvoir d'admonestation et un pouvoir d'amende, comme en dispose déjà son homologue français, la Commission nationale de l'informatique et des libertés (CNIL).

Le récent règlement européen général sur la protection des données[23] reconnaît formellement le « délégué à la protection des données ». Cette fonction figurait déjà dans la directive 95/46 sous les termes « détaché à la protection des données » mais, à la différence de la directive 95/46, le règlement rend cette fonction obligatoire dans certaines hypothèses.

Le règlement rend obligatoire l'engagement de délégués à la protection des données dans le secteur public, ce qui est une bonne chose. Chaque institution publique doit ainsi désigner un délégué à la protection des données mais, en fonction de leur structure organisationnelle et de leur taille, plusieurs institutions publiques peuvent désigner un délégué à la protection des données qui leur est commun.

Le délégué à la protection des données est une personne qui doit veiller à la légalité des traitements de données effectués par le responsable de traitement ou le sous-traitant qui l'a désigné. Il est également le point de contact des citoyens pour toutes les questions relatives à l'utilisation de leurs données à caractère personnel. En toute hypothèse, il doit agir de manière indépendante, ce qui implique qu'il ne peut recevoir aucune instruction relative à l'exécution de ses missions.

Engager un délégué à la protection des données présente un réel intérêt. Ce rôle est d'ailleurs obligatoire depuis plusieurs années en Allemagne, notamment, et y est perçu très positivement. Le groupe européen dénommé « Article 29 » sur la protection des données fait même état du fait qu'en Allemagne, « de l'avis général, c'est essentiellement

22. L., 8 déc. 1992, art. 32, sur la protection de la vie privée à l'égard des traitements de données à caractère personnel.
23. Pour accéder à ce texte : *http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679*

aux détachés à la protection de la vie privée que l'on doit le succès de la protection des données. Une nouvelle profession a été créée, avec sa propre formation et d'importantes activités d'échange d'informations sous la forme de congrès, de séminaires, de périodiques et d'autres publications ». D'ailleurs, « le secteur allemand de la protection des données a prouvé son efficacité lors de la consultation de la Commission sur la mise en œuvre de la directive. Près de 50 % de toutes les réponses fournies venaient d'Allemagne[24] ».

Le délégué à la protection des données constitue un réel apport pour l'institution qui l'engage. D'une part, il prend en charge l'ensemble des questions, souvent complexes, liées à la légalité des traitements de données effectués par le responsable de traitement ou le sous-traitant. Il veille notamment à réguler les accès aux données, à enregistrer les différentes informations relatives à l'utilisation des données, à mettre en place les outils de sécurité informatique nécessaires contre le piratage, etc. Il est également un interlocuteur privilégié de la Commission de la protection de la vie privée afin, notamment, de lui faire état des difficultés juridiques soulevées par les traitements de données menés au sein de son institution et d'être tenu au courant de ses recommandations en la matière.

D'autre part, le délégué à la protection des données est également le point de contact des citoyens qui souhaitent accéder à leurs données, en obtenir une copie, recevoir des explications sur les utilisations qui en sont faites. Peu exercés jusqu'à présent, ces droits sont renforcés par le règlement en projet. Il y a donc lieu de s'attendre à ce que les citoyens soient encouragés à les exercer, générant par là du travail supplémentaire pour le responsable de traitement ou le sous-traitant sollicité qui seront soulagés de pouvoir s'appuyer sur le délégué à la protection des données.

Conclusion

La Belgique a développé un modèle inédit d'administration en réseaux, fondé sur la réutilisation maximale des données à caractère personnel des citoyens. L'objectif est la collecte unique des données des citoyens tout en veillant à la protection de leur vie privée.

Les données à caractère personnel sont stockées dans des sources authentiques de données, placées sous la responsabilité de diverses administrations. Elles sont ensuite échangées, entre les administrations qui en ont besoin, grâce à un intégrateur de services.

24. Groupe de l'article 29 sur la protection des données, *Rapport sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne*, 18 janv. 2005, WP 106, p. 19.

Ce modèle d'administration électronique présente de nombreux avantages en termes d'efficacité et de simplification administrative. Il génère aussi des craintes. Pour contrer ces dernières, divers moyens de contrôle existent, de manière à permettre à chacun de comprendre et de contrôler l'État dans l'univers numérique de plus en plus opaque.

Références bibliographiques

Bundshuch-Rieseneder F., *"Governance and E-Governance in the Frame of Bologna Process", in* Come T. et Rouet G., *Bologna Process, European Construction, European Neighbourhood Policy*, 2011, Bruxelles, Bruylant, p. 253 et 254.

Degrave É., *L'e-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, 2014, Bruxelles, Larcier, coll. « Crids », nos 40 et s.

Dinant J.-M., Lazaro C., Poullet Y., Lefever N. et Rouvroy A., « L'application de la Convention 108 au mécanisme de profilage. Éléments de réflexion destinés au travail futur du Comité consultatif », *T-PD*, mars 2008, 01, p. 5.

Duaso Calès R., *Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau*, thèse, sept. 2015, université de Montréal et université Panthéon-Assas Paris II, sept. 2011, p. 37 à 44.

Hildebrandt M., *"Who is Profiling Who? Invisible Visibility", in* Gutwirth S., Poullet Y., De Hert P., de Terwangne C. et Nouwt S. (dir.), *Reinventing Data Protection?*, 2009, Dordrecht, Springer, p. 241.

Maisl H., « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », *in* Chatillon G. et du Marais B. (dir.), *L'administration électronique au service des citoyens*, 2003, Bruxelles, Bruylant, p. 349 à 359.

Papakonstantinou V., *"A Data Protection Approach to Data Matching Operations Among Public Bodies", International Journal of Law and Information Technology* 2001, vol. 9, n° 1, p. 62-63.

Solove D., *"I've Got Nothing to Hide' and Other Misunderstandings of Privacy", San Diego Law Review* 2007, vol. 44, 745, p. 745-772.