Privacy by design et e-gouvernement

Degrave, Élise; Vanderose, Benoît

Published in:
Pyramides. Revue du Centre d'études et de recherches en administration publique (U.L.B.)

Publication date:
2013

Document Version
le PDF de l'éditeur

PRIVACY BY DESIGN ET *E-GOUVERNEMENT* : UN MODÈLE INÉDIT EN BELGIQUE[1]

Elise DEGRAVE[2] ***et Benoît VANDEROSE***[3]

Résumé

Les technologies de l'information et de la communication ont ouvert de nouvelles perspectives dans le secteur public, au service de la qualité et de l'efficacité des missions administratives accomplies. Pour protéger la vie privée des citoyens dont les nombreuses données à caractère personnel sont enregistrées et réutilisées, tout en ne nuisant pas à l'efficacité administrative, la Belgique a fait application du concept de « privacy by design ». Elle l'a concrétisé en mettant en place un modèle inédit d'administration « en réseaux » fondé sur la décentralisation des données enregistrées.

[1] Cette contribution est inspirée des articles suivants : Vanderose, Degrave and Habra (2015, pp. 210-215) et Degrave (2015, pp. 518 à 536).

[2] E. Degrave, Chargée de cours à la Faculté de droit de l'Université de Namur ; chercheuse à la Chaire E-gouvernement de l'Université de Namur et au Centre de recherches Information Droit et Société (CRIDS).

[3] B. Vanderose, Maître de conférence à la Faculté d'informatique de l'Université de Namur ; chercheur à la Chaire E-gouvernement de l'Université de Namur et au centre Precise.

I. Introduction

Aujourd'hui, l'administration est engagée dans l'ère de l'*electronic government* ou « e-gouvernement », que l'on appelle aussi « administration électronique ». Ce terme générique désigne l'ensemble des utilisations des technologies de l'information et de la communication dans l'administration, ainsi que les mutations que ces utilisations y engendrent[4].

Comment utiliser les technologies pour renforcer au maximum l'efficacité de l'administration ? Certes, l'informatisation de l'administration aboutit à remplacer les fichiers papier par des bases de données électroniques, l'envoi de courriers postaux par des courriels, etc.

Mais il y a plus. Depuis toujours, l'administration collecte une masse d'informations personnelles sur chaque citoyen : l'adresse, l'âge, la composition de famille, l'état de santé, les numéros de comptes bancaires, le revenu cadastral de l'habitation, la plaque d'immatriculation, ... sont autant d'informations très diverses dont l'administration doit disposer pour exécuter ses missions légales.

Avant le développement de l'e-gouvernement, dans le contexte de l'administration dite « de papier », chaque institution publique œuvrait de manière cloisonnée, collectait auprès des citoyens les informations dont elle avait besoin pour l'exécution de ses propres missions et ne les partageait pas ensuite. 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. Le citoyen pâtissait également de cette situation, 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.

---

[4] E. Degrave, 2014, p. 33. Voy. égal. les éléments les plus pertinents mentionnés dans différentes descriptions de l'e-gouvernement repris dans les documents suivants : Commission des Communautés européennes, 26 septembre 2003, p. 4 ; Commission des Communautés européennes, 1998, p. 8 ; Observatoire des Droits de l'Internet, 2003 ; Banque mondiale, « Definition of E-Government » ; Silcock, 2001, p. 88 ; De Roy, de Terwangne et Poullet, 2007, p. 310 ; Boudry, De Rynck, Janssens et Rotthier, 2009, pp. 1 et 2 ; Chatillon, 2011, pp. 28 et 29 ; Bundshuch-Rieseneder, 2011, p. 260.

Aujourd'hui, il est possible, grâce aux technologies, de concrétiser l'objectif de collecte unique des données. L'idée est de faire en sorte que le citoyen n'ait à communiquer ses informations qu'une seule fois à l'administration, à charge pour cette dernière de faire circuler ces informations entre les institutions qui en ont besoin.

II. Structure de l'administration et *Privacy by design*

II.1. Centralisation ou décentralisation des données ?

Pour atteindre l'objectif de collecte unique des données qui facilite tant les tâches du citoyen que celles de l'administration, une réorganisation structurelle de l'administration est nécessaire. En particulier, il y a lieu de s'interroger sur la manière dont les données à caractère personnel des citoyens seront collectées, stockées et réutilisées.

A cet égard, deux modèles d'organisation de l'administration retiennent notre attention.

Le premier modèle est celui de la *centralisation des données* dans une seule base de données placée au cœur de l'administration. Dès qu'une institution publique a besoin d'une information relative à un citoyen, il lui suffit de se connecter à la base de données et d'y prendre l'information recherchée.

Ce modèle a été envisagé en France, dans les années soixante-dix. Le projet SAFARI[5] entendait centraliser les données de chaque citoyen français. Rapidement qualifié de « SAFARI ou la chasse aux Français », ce projet a généré beaucoup de critiques. On y a vu une menace importante pour la protection de la vie privée des citoyens et la sécurité des données informatiques.

Pour répondre à ces préoccupations, le second modèle est celui de la *décentralisation des données*. Ce modèle a été pensé en tenant compte de l'importance de protéger la vie privée des citoyens dans la conception même de la structure administrative, tout en veillant à faciliter l'efficacité du travail administratif. Dans ce modèle, les données des citoyens sont réparties entre plusieurs administrations. Parallèlement à cet enregistrement décentralisé des données, des outils sont mis en place pour permettre l'échange des

[5] SAFARI pour « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus ».

données entre les administrations qui en ont besoin. Grâce à la décentralisation des données, on diminue fortement les risques d'atteinte à la vie privée des individus puisque le regroupement des données d'un citoyen est rendu très complexe.

Ce modèle a été mis en place en Belgique, au départ de la création de la Banque Carrefour de la sécurité sociale. Nous y reviendrons dans les lignes qui suivent.

II.2. Le concept de Privacy by design

Tenir compte de la protection de la vie privée dès la conception de la structure de l'administration rejoint le concept de *Privacy by design*[6]. Ce concept émerge du constat que, bien souvent, les instruments législatifs ne sont pas suffisants pour encadrer correctement la protection de la vie privée à l'égard des traitements de données à caractère personnel. Les règles existent, mais elles sont difficilement respectées ou s'avèrent mal adaptées à l'e-gouvernement.

Privacy by design désigne la méthode qui consiste à intégrer la protection de la vie privée en amont, dans la conception même du système informatique, plutôt que de créer ce système et de penser seulement ensuite à protéger la vie privée par des normes[7]. Pour le dire autrement, il s'agit de créer des outils qui, en eux-mêmes, présentent des garanties de protection pour la vie privée des personnes concernées. De cette manière, la protection de la vie privée est soutenue par la technique, en sus d'être organisée par des normes. Ensemble, ils constituent *« un rempart efficace contre les excès rendus possibles par le progrès »*[8].

Le concept de *Privacy by design* reçoit de plus en plus d'importance dans le régime de la protection de la vie privée et des données à caractère personnel. En 2010, elle a fait l'objet d'une résolution adoptée par les commissaires à la

[6] Cette idée a été développée dans les années quatre-vingt dix par Ann Cavoukian, commissaire à la protection de la vie privée de l'Ontario, au Canada, qui y consacre un site internet (www.privacybydesign.ca). Voy. Cavoukian, 2009. Voy. aussi Schaar, 2010, pp. 267-274.

[7] Voy. Cavoukian, 2009, p. 3 ; Le Clainche, 2010, pp. 166 à 169 ; Groothuis, 2009, p. 240.

[8] Le Clainche, 2010, p. 168.

protection des données et de la vie privée[9]. Cette résolution définit la notion de *Privacy by design* comme « *the philosophy and approach of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle* »[10].

Depuis lors, le concept de *Privacy by design* est intégré dans le projet de règlement sur la protection des données[11]. Ainsi, l'article 23.1 affirme que *« le responsable du traitement applique, tant lors de la définition des moyens de traitement que lors du traitement proprement dit, les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée »*. Elle a dès lors vocation à devenir une exigence contraignante pour tous les responsables de traitements, qui devront mettre en œuvre des mesures techniques garantissant, en amont, le respect des règles de protection des données.

III. Le modèle d'e-gouvernement belge

III.1. Un modèle inédit

Pour mettre en œuvre efficacement l'échange des informations entre administrations, la Belgique s'engage, depuis plusieurs années, dans un modèle d'organisation administrative 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. Pour le dire autrement, les données utilisées sont enregistrées de manière décentralisée au sein de l'administration et échangées entre institutions grâce à un intégrateur de services.

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 ».

---

[9] Resolution on Privacy by design, 32nd International Conference on Data protection and Privacy Commissioners, Jerusalem 27-29 octobre 2010.
[10] Ibidem, p. 2.
[11] A ce sujet, voy. Van Canneyt, 2012, p. 57 ; Gayrel et Robert, 2012, p. 176.

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 »[12]. 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.

[12] Nous revenons ultérieurement plus en détail sur cette notion.

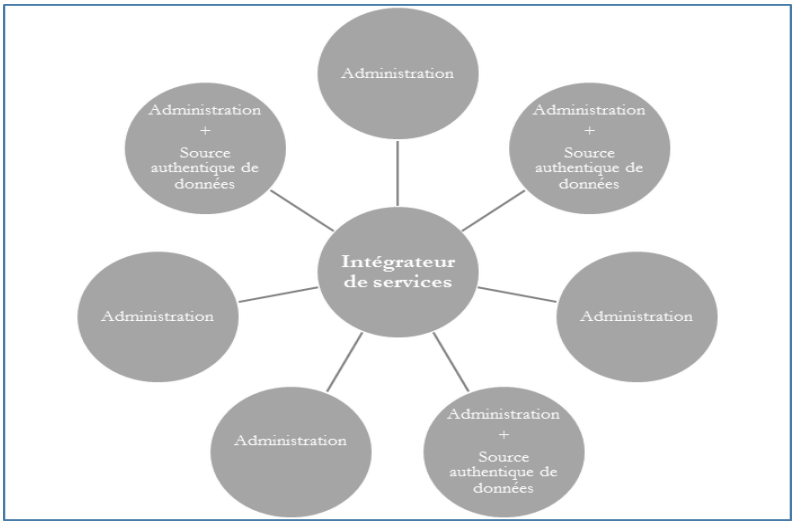


Schéma illustrant un réseau d'administrations composé d'un intégrateur de services auquel sont reliées plusieurs administrations dont certaines détiennent une source authentique de données.

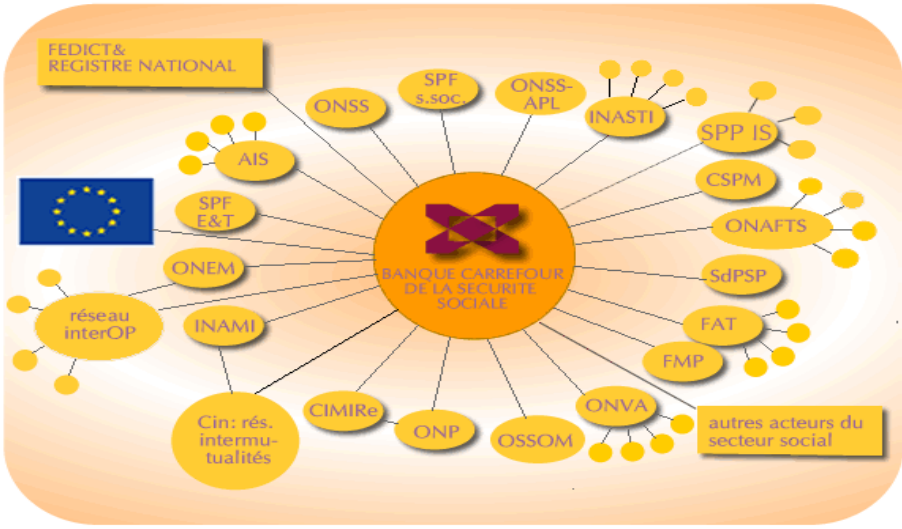
III.2. Plusieurs réseaux d'administrations et intégrateurs de services

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 quatre-vingt-dix[13]. S'en est suivi la

[13] Voy. la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, *MB*, 22 février 1990. Ci-après « loi du 15 janvier 1990 relative à la Banque Carrefour de la sécurité sociale ».

création, en 2008, du réseau sectoriel de la santé, au sein duquel la plate-forme *eHealth* assume le rôle d'intégrateur de services[14].



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, qui sera étudié dans les lignes qui suivent. 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

[14] Voy. la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme *eHealth* et portant diverses dispositions, *MB*, 13 octobre 2008.

institutions de la Communauté flamande et de la Région flamande[15]. 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 au sein duquel œuvre, depuis 2013[16], 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 (Etat fédéral, Communauté française et Région Wallonne, Communauté flamande et Région flamande), sans devoir s'interroger sur le type de données recherché 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 plate-forme *eHealth*.

III.3. Avantages pour l'administration et pour le citoyen

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 « *datawarehouse* » et d'y appliquer des calculs 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 de fraudes[17].

---

[15] Décret du 13 juillet 2012 portant création et organisation d'un intégrateur de services flamand, *MB*, 1er août 2012.

[16] Décret du 4 juillet 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 juillet 2013.

[17] Pour de plus amples précisions sur la technique du profilage, voy. Recommandation CM/Rec(2010)13 du Comité des Ministres du Conseil de l'Europe aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, disponible

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 est également épargné de certaines démarches administratives grâce à l'automatisation des procédures. A cet égard, par exemple, une application informatique créée par 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 Economie ont besoin d'informations relatives à chaque naissance. Jadis, ces administrations obtenaient ces informations via des formulaires en papier envoyés par les hôpitaux. Aujourd'hui, les hôpitaux se connectent au portail *Ebirth*, encodent les données requises, et celles-ci sont acheminées respectivement vers les communes, la Communauté française et le SPF Economie[18].

Ces avantages constituent des critères de qualité proportionnels (ou linéaires) du point de vue d'un utilisateur (citoyen ou agent de l'administration)[19]. Dans les deux cas, la satisfaction de l'utilisateur est directement liée à la mise en place du mécanisme permettant de proposer cette qualité. De par leur nature, ces avantages en termes d'efficacité administrative ne peuvent donc être comparés plus finement afin de distinguer l'ampleur de l'avantage d'un modèle à un autre. De ce fait, ils restent globalement similaires à ceux offerts par un modèle centralisé tel que le coffre-fort électronique.

III.4. Respect des principes de Privacy by Design

Le modèle d'organisation administrative mis en place en Belgique propose un net avantage dans le domaine de la protection des données à caractère personnel. Par opposition au modèle du coffre-fort électronique qui consiste à héberger les données auprès de chaque citoyen concerné, le modèle belge ne dispose pas de point de collecte central constituant un point unique de défaillance. Il est donc impossible pour un acteur tiers malintentionné d'accéder à l'entièreté des données d'un citoyen en un seul accès (autorisé

---

sur le site www.coe.int; Hildebrandt, 2009, p. 241 ; Papakonstantinou, 2001, pp. 62-63 ; Dinant, Lazaro, Poullet, Lefever et Rouvroy, 2008, p. 5 ; Degrave, 2014, pp. 40 et suivantes.

[18] Pour plus d'informations sur *Ebirth*, voy. la présentation générale d'*Ebirth* disponible à l'adresse :
https://www.ehealth.fgov.be/fr/services-en-ligne/ebirth/presentation-d-ebirth

[19] A ce sujet, voy. Sauerwein, Bailom, Matzler and Hinterhuber, « The kano model: How to delight your customers », 1996, pp. 313-327.

ou résultant d'une tentative de piratage). Cette qualité est renforcée par le fait qu'aucun numéro d'identification global n'est mis en place. En effet, un citoyen possède un numéro d'identification propre à chaque réseau ce qui empêche les références croisées d'un réseau à l'autre. Dans les faits, un acteur malintentionné tentant d'accéder aux données d'un citoyen devrait donc mener pour chaque type d'information une tentative d'accès à chaque source authentique de données, ce qui démultiplie l'effort demandé et réduit donc les risques de succès d'une telle tentative. Dans ce modèle, la sécurité physique des données (c'est-à-dire le niveau de résilience des serveurs hébergeant ces données face à des tentatives de piratage) ne peut par contre pas être garantie globalement. Chaque source authentique de données se doit donc de fournir le niveau de sécurité requis afin que l'ensemble du système informationnel demeure résilient. En vertu du modèle organisationnel lui-même, une faille de sécurité au niveau d'une source authentique précise ne permet que d'accéder à une partie très parcellaire de l'information concernant un citoyen.

En termes de protection des données à caractère personnel, c'est bel et bien dans la lutte contre l'utilisation abusive par un acteur interne à l'administration que le modèle excelle. En ce sens, et bien que le modèle ne se revendique pas explicitement d'une approche de type *privacy by design*, il s'agit là d'une application rigoureuse des principes fondamentaux d'une telle approche. En effet, toute approche de type *privacy by design* se doit de respecter les sept principes fondamentaux suivants[20] :

1. prendre des mesures *proactives* et non réactives ; des mesures *préventives* et non correctives ;
2. assurer la protection *implicite* de la vie privée ;
3. *intégrer* la protection de la vie privée dans la conception des systèmes et des pratiques ;
4. assurer une fonctionnalité *intégrale* selon un paradigme à somme positive et non à somme nulle ;
5. assurer la sécurité de bout en bout, pendant *toute la période de conservation des renseignements ;*
6. assurer la *visibilité* et la *transparence ;*
7. *respect* de la vie privée des utilisateurs.

Il est notable que le modèle présenté précédemment se conforme implicitement à ces principes. L'idée de protection des données à caractère

[20] A ce sujet, voy. Cavoukian et al., 2009.

personnel se trouve au centre des préoccupations fondamentales de ce modèle. A l'heure actuelle, la seule limitation majeure au regard de ces principes est le fait que la transparence ne soit pas encore implémentée. En effet, contrairement à une approche de type coffre-fort, les usagers eux-mêmes ne possèdent pas de point d'accès central à leurs données propres, ni sur la nature des échanges de données entre les différentes administrations. Toutefois, cette limitation n'est pas rédhibitoire dans la mesure où la nature décentralisée du modèle n'exclut pas la mise en place d'une « surcouche » informationnelle supplémentaire qui pourrait combler ce manque, par exemple sous la forme d'un portail personnel accédant de façon transparente aux données utiles au travers de l'intégrateur de services. Un tel portail serait une implémentation possible permettant de conserver les avantages en termes de protection tout en garantissant le droit à l'information et à la transparence.

Conclusions

Alors que la protection de la vie privée peut sembler être un obstacle à l'efficacité administrative, le modèle belge d'e-gouvernement démontre qu'il est possible d'organiser une administration à la fois efficace et respectueuse de la protection de la vie privée. Ce modèle a d'ailleurs été pensé au départ des préoccupations de protection de la vie privée des citoyens, ce que l'on appelle le « privacy by design ».

Les perspectives offertes par l'administration électronique belge sont prometteuses. Elles permettent aux citoyens et à l'administration de gagner du temps et de l'argent, grâce à un allègement considérable des démarches administratives et à un gain d'efficacité dans les tâches accomplies.

L'automatisation de l'octroi de certains droits, l'informatisation de la lutte contre la fraude fiscale et sociale, l'accès à des formulaires en ligne partiellement préremplis, une information claire et transparente disponible 24h sur 24 et 7 jours sur 7 sont autant d'exemples du succès grandissant du nouveau mode de relation entre l'administration et ses usagers.

Bibliographie

Banque mondiale, « Definition of E-Government », http://web.worldbank.org

Boudry, E., De Rynck, F., Janssens, S. en Rotthier, S., *E-government : nieuwe kans of nieuw probleem*, Bruges, die Keure, 2009.

Bundshuch-Rieseneder, F., « Governance and e-governance in the frame of Bologna Process », *in Bologna Process, European Construction, European Neighbourhood Policy* (T. Come et G. Rouet dir.), Bruxelles, Bruylant, 2011.

Chatillon, G., « Fondements, principes et nature du droit de l'administration électronique », in : *Droit de l'administration électronique. De nouveaux droits pour les usagers. Des nouvelles règles pour les agents* (G. Chatillon dir.), Bruxelles, Bruylant, 2011.

Cavoukian, A., « Privacy by design, take the challenge », *Information and Privacy Commissioner of Ontario*, Canada, 2009.

Cavoukian, A., « Privacy by design: The 7 foundational principles », *Information and Privacy Commissioner of Ontario*, Canada, 2009.

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

Commission des Communautés européennes, « Le rôle de l'administration en ligne (eGovernment) pour l'avenir de l'Europe », COM(2003) 567 final, du 26 septembre 2003.

Commission des Communautés européennes, « L'information émanant du secteur public : une ressource clef pour l'Europe. Livre vert sur l'information émanant du secteur public dans la société de l'information », COM(1998)585, p. 8.

Degrave, E., *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier, coll. Crids, 2014.

Degrave, E., « L'intégrateur de services fédéral au cœur de la simplification administrative », *A.P.*, 2015, pp. 518 - 536.

De Roy, D., de Terwangne, C. et Poullet, Y., « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », *C.D.P.K.*, 2007.

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

Gayrel, C. et Robert, R., « Proposition de règlement sur la protection des données – premiers commentaires », *J.T.*, 2012.

Groothuis, M, « De digitale overheid en de menselijke maat », *Computerrecht*, 2009.

Hildebrandt, M., « Who is Profiling Who ? Invisible Visibility », *in Reinventing Data Protection ?* (Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. ed.), Dordrecht, Springer, 2009.

Le Clainche, J., « Consentement et traitements de données à caractère personnel », *in Les technologies de l'information au service des droits : opportunités, défis, limites* (Le Métayer, D. dir.), Bruxelles, Bruylant, 2010.

Observatoire des Droits de l'Internet, « Facteurs de succès de l'e-gouvernement. Avis n°2 », décembre 2003, disponible sur le site http://www.internet-observatory.be

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.

Sauerwein, E., Bailom, F., Matzler, K. and Hinterhuber, H.H., « The kano model: How to delight your customers », *International Working Seminar on Production Economics*, 1996, vol. 1.

Schaar, P., « Privacy by design », *Identity in the Information Society*, 2010.

Silcock, R., « What is e-government ? », *Parliamentary Affairs*, 2001, vol. 54.

Van Canneyt, T., « Naar meer efficiënte bescherming van persoonsgegevens – een beknopte bespreking van het voorstel voor een verordening van de Europese commissie », *Cah. Jur.*, 2012/2.

Vanderose, B., Degrave, E. and Habra, N., « Privacy by design and administrative efficiency in e-governance : a case study », *CEUR Workshop Proceedings*, CEUR-WS, 1420, 2015.