Le règlement général sur la protection des données et le secteur public

Degrave, Élise

Published in:
Revue de droit communal

Publication date:
2018

Document Version
le PDF de l'éditeur

Le règlement général sur la protection des données et le secteur public

Élise DEGRAVE[1]
Chargée de cours à la Faculté de droit de l'UNamur
Codirectrice de la Chaire Egov/Crids

TABLE DES MATIÈRES

I. Prélude

1. Le contexte – Les agents de l'administration le savent mieux que quiconque : depuis quelques années, le secteur public est pleinement engagé dans la voie de l'administration numérique, dite aussi « administration électronique » ou « e-gouvernement ».

Dans les murs des administrations, on entend désormais parler de « cloud », de « banque-carrefour », de « réseaux sociaux », de « diffusion en ligne », de « sources authentiques de données », de « données à caractère personnel », de « cyberattaques », … Les citoyens eux-mêmes, conscientisés et dès lors un peu craintifs, saisissent les administrations de préoccupations nouvelles sur les données conservées à leur sujet, la raison et la durée de cette conservation, l'identité des personnes qui y ont eu accès, leur souhait de faire supprimer certaines données. Il faut dire que, pour eux aussi, l'administration numérique représente un bouleversement important. Notamment parce qu'ils ne disposent plus de dossier administratif en papier. À la faveur de la simplification administrative, celui-ci est remplacé par un ensemble de données à caractère personnel disséminées dans une multitude de bases de données dénommées « sources authentiques de données ». Pour tout un chacun, la consultation du « dossier administratif » est devenue complexe, opaque, intangible, … à l'image de l'univers numérique dans son ensemble.

Dans ce contexte nouveau, l'enjeu fondamental de l'administration électronique est de garder la confiance du citoyen, sans quoi, aucune collaboration n'est plus possible.

2. Le RGPD – C'est en tenant compte notamment de cet enjeu qu'a été rédigé le Règlement européen sur la protection des données à caractère personnel (ci-après « RGPD »), destiné à encadrer les traitements de données à caractère personnel, tant dans le secteur privé que dans le secteur public.

Ce texte est très long. 200 pages, 99 articles. Il est le fruit de plus de quatre années de négociations difficiles. Adopté par le Parlement européen et le Conseil, il est entré en vigueur le 24 mai 2016. Il sera d'application à partir du 25 mai 2018, sans qu'une transposition dans les législations nationales soit nécessaire. Le choix d'un règlement plutôt que d'une directive est justifié par la volonté d'imposer un corps de règles identiques aux 28 États membres de l'Union européenne[2].

Ce texte poursuit plusieurs objectifs. Deux d'entre eux intéressent particulièrement l'administration.

D'une part, il importe de renforcer la *transparence* dans les traitements de données. Les citoyens ont le droit d'y voir clair à propos des données collectées à leur sujet par l'administration, l'utilisation qui en est faite par la suite, pour quelles raisons, etc. Appliqué au secteur public, cet impératif prolonge le mouvement d'ouverture de l'administration vers les citoyens, mouvement engagé à la faveur, notamment, de la consécration du droit fondamental à la transparence administrative[3], de l'adoption de la loi du 11 avril 1994 sur la publicité de l'administration[4] et de la loi du 12 novembre 1997 relative à la publicité de l'administration dans les provinces et

1. L'auteure remercie Yasmine Ourari, Juriste à E-wbs et à la BCED, Marie-Laure Van Rillaer, Juriste à l'UVCW ainsi que Loïck Gérard, Assistant à la Faculté de droit de l'UNamur et Chercheur à la Chaire Egov/Crids, pour les idées et opinions échangées. Toutefois, les propos ici affirmés n'engagent qu'elle-même.
2. Pour une synthèse de l'historique du RGPD, voir V. VERBRUGGEN, « Mise en œuvre du Règlement général sur la protection des données : coup de projecteur sur certaines nouvelles obligations à charge des responsables de traitement et des sous-traitants », *Orientations,* 2017, pp. 2 à 4.
3. Art. 32 de la Constitution.
4. Pour plus d'informations à ce sujet, voir E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* Bruxelles, Larcier, 2014, n^{os} 240 et s.

les communes. C'est l'idée que le temps est révolu d'une administration secrète et distante, se réfugiant derrière l'opacité de son action. Des puits de lumière sont à présent creusés dans cette forteresse. Ceux-ci doivent permettre au citoyen de savoir et de comprendre ce qu'il se passe derrière les murs de l'administration, notamment s'agissant de l'utilisation des données qu'il a confiées aux pouvoirs publics. Fort de cette prise de conscience, le citoyen peut ainsi participer en pleine connaissance de cause au processus démocratique, et établir une relation de confiance avec l'administration.

D'autre part, le RGPD veut renforcer la *responsabilisation* des acteurs, que l'on désigne également par le terme « accountability ». À présent, les responsables de traitement doivent non seulement respecter le régime juridique de la protection des données mais également être en mesure de démontrer à tout instant ce respect à l'autorité de protection des données[5]. Un changement de culture va ainsi être provoqué au sein du secteur public puisque, pour répondre à cet objectif, l'administration responsable de traitement devra notamment tenir un « registre des activités de traitements », qui doit l'amener à se poser certaines questions cardinales avant la mise en place d'un traitement de données effectif et à effectuer une « analyse d'impact » visant à anticiper les failles de sécurité. Nous y reviendrons dans cette étude.

3. Une évolution mais pas une révolution – Quant au contenu de ce texte, quoi qu'en disent les apparences, le RGPD n'est pas une révolution. C'est une évolution de la directive 95/46, qui, en Belgique, a été transposée dans la loi du 8 décembre 1992. En effet, nombre d'obligations imposées par le RGPD étaient déjà prévues par la directive 95/46 et le régime juridique belge de protection des données et étaient censées être appliquées par les administrations. Le RGPD fait donc office de « piqûre de rappel » de ces règles, mais il s'agit d'un rappel bien nécessaire car certaines règles n'étaient pas ou peu appliquées jusqu'ici.

Parmi les obligations nouvelles émanant du RGPD, certaines ne s'appliquent pas au secteur public. Tel est le cas du droit à la portabilité des données, qui ne s'applique pas « au traitement 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 »[6]. Il en va de même du droit à l'effacement, plus connu sous le nom de « droit à l'oubli », qui ne s'applique pas lorsque le traitement est nécessaire « pour respecter une obligation légale qui requiert le traitement prévu par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement »[7].

Par contre, d'autres obligations pourraient entraîner de véritables changements dans la culture de l'administration. C'est le cas de la désignation d'un délégué à la protection des données, de la tenue d'un registre des activités de traitement et de l'élaboration d'une analyse d'impact, obligations sur lesquelles se concentrent les lignes qui suivent.

4. Les conséquences du RGPD sur le cadre normatif actuel – Jusqu'au 28 mai 2018, le cadre normatif de la protection des données à caractère personnel est composé des règles éparses en vigueur pour le moment.

L'assise de la matière est la *directive 95/46 UE*, transposée en Belgique par la *loi du 8 décembre 1992* relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

À cette loi fédérale s'ajoutent, pour le secteur public, des *lois sectorielles*, parmi lesquelles on retrouve, entre autres, la loi du 8 août 1983 sur le Registre national, la loi du 15 janvier 1990 sur la Banque-carrefour de la sécurité sociale et la loi du 21 août 2008 sur la plateforme « *e-health* ».

Des *décrets et ordonnances* complètent l'arsenal normatif des Communautés et des Régions, tels que le décret de la Communauté française et de la Région wallonne, du 10 juillet 2013, portant assentiment à l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, le décret flamand du 18 août 2008 relatif à l'échange électronique de données administratives, l'ordonnance bruxelloise du 8 mai 2014 portant création et organisation d'un intégrateur de services régional, etc.

Le 28 mai 2018, le RGPD entre en application sans qu'il faille attendre une transposition législative en droit belge. Ainsi, dès ce jour, la directive 95/46 et la loi du 8 décembre 1992 seront supprimées. Se pose alors la question du devenir des lois sectorielles précitées et des décrets et ordonnances applicables à l'administration électronique belge. C'est pour rencontrer ces particularités, notamment, qu'une loi-cadre est en cours de rédaction, qui viendra compléter le RGPD en Belgique.

Signalons aussi que la Commission de la protection de la vie privée est substantiellement réformée et

5. V. VERBRUGGEN, *op. cit.*, p. 5 ; C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, p. 28.
6. Art. 20 RGPD.
7. Art. 17 RGPD.

rebaptisée « Autorité de protection des données ». La loi du 3 décembre 2017 portant création de l'Autorité de protection des données a été publiée au *Moniteur belge* le 10 janvier. Ce texte prévoit notamment la suppression des comités sectoriels qui, jusqu'ici, autorisaient les échanges de données entre administrations. Pour autant, et de manière assez inquiétante, le texte ne précise pas quel autre contrôle sera mis en place. En outre, l'autorité de protection des données se voit dotée du pouvoir de sanctionner les responsables de traitement en leur imposant une amende dont le montant peut aller jusqu'à 20 millions d'euros[8]. S'agissant du secteur public, le RGPD précise toutefois que « chaque Etat membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire ». Peut-être la future loi-cadre belge concrétisera-t-elle cette possibilité ?

La présente étude entend éclairer les administrations qui se préparent à l'entrée en application du RGPD, sans pour autant prétendre à l'exhaustivité. Il s'agit, après un bref rappel des acteurs et des données soumis au RGPD, de mettre en évidence trois nouvelles obligations qui s'imposent aux administrations et pour lesquelles une préparation utile peut d'ores et déjà être entamée.

II. Les acteurs et les données soumis au RGPD

5. Les acteurs : le responsable de traitement et le sous-traitant – Le RGPD impose des obligations tant au responsable de traitements qu'au sous-traitant.

Au sein du secteur public, le *responsable de traitement* est « la personne morale, l'autorité publique[9], le service ou un autre organisme qui seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Concrètement, différentes hypothèses doivent être envisagées.

Soit une norme de valeur législative ou réglementaire désigne explicitement le responsable du traitement. Par exemple, en vertu du Code wallon de l'action sociale et de la santé, la Direction générale opérationnelle Pouvoirs locaux, Action sociale et Santé est le responsable du traitement consistant en la collecte de données relatives aux opérateurs de la politique de l'action sociale et de la santé[10].

Soit le traitement de données résulte de la décision d'un organe d'une administration, tel qu'un conseil communal, par exemple. Dans ce cas, c'est l'organe décideur qui est le responsable du traitement[11]. Par exemple, comme l'affirme la Commission de la protection de la vie privée[12], le conseil communal est le responsable du traitement des données collectées dans le cadre des sanctions administratives communales, étant donné qu'il décide des sanctions administratives contre les infractions à ses règlements et ordonnances[13].

Soit le traitement de données a été décidé au niveau d'un service, tel que le service de l'État civil qui déciderait d'enregistrer les personnes ayant demandé certains documents. Dans ce cas, le responsable du traitement est l'organe ou la personne ayant le pouvoir de décider de ce traitement[14].

Le *sous-traitant* est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement ». Par exemple, sont susceptibles d'être des sous-traitants, les prestataires de service informatique, qui assurent l'hébergement et la maintenance du service[15], une société spécialisée dans la sécurité informatique, un intégrateur de logiciel qui accompagnerait l'administration dans l'utilisation et la personnalisation d'un logiciel, etc. *A contrario,* dans la mesure où ils ne traitent pas des données à caractère personnel, un fabricant de matériel informatique tel qu'un fabricant de badges d'accès au bâtiment, ou un éditeur de logiciel, qui assure la conception et la commercialisation d'un logiciel, ne sont pas des sous-traitants.

L'administration qui recourt à un sous-traitant doit veiller à ce que ce dernier « présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du [RGPD] et garantisse la protection des droits de la personne

8. Voir art. 83 RGPD.
9. Il est à noter que la notion d'autorité publique n'est pas définie par le Règlement, ce qui risque d'ouvrir la porte à des questions d'interprétation au cas par cas si la future loi-cadre belge manquait à la définir.
10. Art. 44/1 du titre 1er du livre IV du Code wallon de l'action sociale et de la santé.
11. Cellule TIC de la DGPL, *Le traitement de données à caractère personnel par l'administration communale : les chartes d'utilisations des ressources informatiques communales*.
12. CPVP, Recommandation n° 04/2010 du 19 mai 2010, concernant la législation relative aux sanctions administratives communales et la protection des données à caractère personnel, nos 45 et 46.
13. Art. 119*bis*, § 1er, de la nouvelle loi communale.
14. Cellule TIC de la DGPL, *Le traitement de données à caractère personnel par l'administration communale : les chartes d'utilisations des ressources informatiques communales*.
15. Pour information, un sous-traitant qui héberge un service informatique met à disposition de ses clients – une administration, par exemple – ses serveurs sécurisés. Il y installe les logiciels souhaités par ses clients, leur site web, les langages de programmation demandés. Il effectue la maintenance, telles que les mises à jour de sécurité et la réparation des serveurs en cas de panne.

concernée »[16]. Il faut donc s'assurer, entre autres nombreux éléments[17], que les employés du sous-traitant sont soumis à une obligation de confidentialité, que les outils proposés par le sous-traitant ne traitent que les données nécessaires à la réalisation des finalités poursuivies et que les mesures de sécurité mises en place sont adaptées aux risques qu'une violation de données à caractère personnel soit commise. En outre, un contrat doit être conclu entre le responsable de traitement et le sous-traitant, qui définit les missions de ce dernier, puisque le sous-traitant ne peut agir que sur instruction du responsable de traitement[18].

6. Les données : les données à caractère personnel – Le RGPD ne s'applique qu'aux traitements de *données à caractère personnel*, notion définie comme « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée 'personne concernée') », une « personne physique identifiable » étant « une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

L'adresse d'un citoyen, sa plaque d'immatriculation, son numéro de compte bancaire, son numéro de téléphone, son adresse mail, les données cadastrales de son habitation, son numéro d'identification au Registre national, ses empreintes digitales sont autant de données à caractère personnel dont l'usage par l'administration est soumis au RGPD.

Le régime juridique spécifique auxquelles sont soumises les données à caractère personnel impose de réévaluer des pratiques parfois très anciennes au sein des administrations[19]. On pense notamment à la publication des naissances, mariages et décès dans le bulletin communal, ou aux informations contenues dans les annonces de projets et les enquêtes publiques.

En effet, une publication numérique ne peut être assimilée à une publication en version papier. La première a un champ de diffusion nettement plus large, qu'offre l'internet. En outre, les moteurs de recherche en ligne permettent de retrouver des informations contenues dans les publications numériques beaucoup plus aisément qu'une fouille manuelle dans les dossiers papier de l'administration.

C'est pourquoi, un bulletin communal déposé dans la boîte aux lettres des citoyens de la commune n'équivaut pas à sa mise en ligne sur le site internet de la commune. De même, l'affichage d'une enquête publique ou d'une annonce de projet aux abords du terrain à bâtir, n'équivaut pas à la mise en ligne de cette même enquête ou annonce sur le site internet de la commune. Lorsque les informations concernées sont accessibles par internet, en format numérique, celles-ci doivent respecter les exigences cardinales du régime juridique de la protection des données à caractère personnel, parmi lesquelles figure notamment le fait de n'utiliser que les données nécessaires à l'objectif poursuivi et de recueillir, le cas échéant, le consentement des citoyens dont les données sont traitées.

Certaines communes l'ont déjà bien compris. Elles ne publient les mariages, naissances et décès, qu'après avoir obtenu le consentement des personnes concernées ou de leur représentant[20]. Quant aux enquêtes publiques et annonces de projet en ligne, seules les données relatives à la construction ou à la transformation du bâtiment concerné sont nécessaires pour recueillir l'avis du voisinage. Nul besoin de connaître l'identité du couple qui mène ledit projet, par exemple[21].

III. L'analyse de trois obligations nouvelles pour les administrations

7. Cas concret[22] – Ainsi qu'on l'a dit, trois nouvelles obligations pour les administrations retiennent l'attention dans cette étude. Il s'agit de l'engagement d'un délégué à la protection des données, de la tenue d'un registre des activités de traitement et de la rédaction d'une analyse d'impact relative à la protection des données.

Commençons l'analyse de ces obligations par un cas concret qui illustrera la suite du propos[23].

Pour stimuler le commerce local et promouvoir les activités touristiques, une ville met en place une application pour smartphone, dénommée « *City Shopy* », que les citoyens sont invités à télécharger. Cette

16. Art. 28 RGPD.
17. Pour le surplus, nous renvoyons au guide efficace conçu par la CNIL (France), et accessible ici www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf.
18. Art. 28, 3, a), RGPD.
19. À vrai dire, cette réévaluation aurait déjà dû être faite dès l'entrée en vigueur de la loi du 8 décembre 1992 qui fixait déjà les balises de l'utilisation des données à caractère personnel. Raison pour laquelle, à cet égard, le RGPD est une piqûre de rappel.
20. Pour un exemple, voir www.nivelles.be/faq/article/97-je-souhaite-que-mon-mariage-la-naissance-de-mon-enfant-ou-le-deces-d-un-proche-soit-mentionne-e-dans-la-rubrique-etat-civil-du-bulletin-communal-gens-de-nivelles.html.
21. Pour un exemple, voir www.liege.be/urbanisme/annonces-de-projet-et-enquetes-publiques-en-cours.
22. Ces trois obligations nouvelles sont également analysées par V. VERBRUGGEN dans son article précité, analyse qui reprend également des développements relatifs aux préoccupations du secteur privé.
23. Ce cas est inspiré du schéma de synthèse relatif à l'analyse d'impact fourni par la CNIL, « PIA. Vue d'ensemble des obligations et de la méthode », accessible ici : www.cnil.fr/sites/default/files/thumbnails/image/171002_fiche_risque_fr_screen_rgb.jpg ainsi que d'un projet dans au moins une commune belge.

application permet de géolocaliser les personnes quand elles se promènent en ville. Lorsqu'elles passent aux abords de certains lieux, elles reçoivent une publicité sur leur smartphone, qui leur signale une promotion dans tel magasin, le nouveau menu de tel restaurant qu'elles ont fréquenté le mois passé, l'ouverture d'une nouvelle boulangerie à proximité, des réductions au musée tout proche, un point de vue à ne pas manquer, etc.

Les citoyens de cette ville aiment beaucoup cette application et la téléchargent massivement. Leurs données sont enregistrées sur un serveur informatique.

Un jour, ce serveur est piraté par une organisation criminelle. Les pirates informatiques accèdent aux données de géolocalisation et d'identification des personnes ayant téléchargé cette application. Ils parviennent à trouver l'adresse de ces personnes et à déduire leurs absences des informations de géolocalisation. Plusieurs personnes sont alors cambriolées.

Cette situation ne plaît ni à la ville ni à ses citoyens.

Comment l'éviter ? C'est ici que l'analyse d'impact révèle tout son sens pour anticiper de tels risques[24].

Au préalable, comment encadrer cet outil pour y voir clair sur l'ensemble des éléments qui le constituent ? Le délégué à la protection des données est un acteur clé de telles pratiques[25] et le registre des activités de traitement, un outil important pour les encadrer[26].

A. La désignation d'un délégué à la protection des données (art. 37 à 39 RGPD)

8. Une obligation dans l'administration – Vérifier que les règles de protection des données sont respectées, remplir les documents adéquats, répondre aux questions des citoyens au sujet de l'utilisation de leurs données, sont autant de tâches déduites du RGPD, pouvant représenter une charge de travail importante, qui vient s'ajouter aux autres missions de l'administration.

Dorénavant, ces tâches seront confiées à un délégué à la protection des données[27], appelé plus généralement « DPO » pour *Data protection Officer*. En effet, l'engagement d'un DPO est désormais obligatoire pour chaque autorité publique et chaque organisme public[28] qui traite des données à caractère personnel, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle.

En l'espèce, la ville ayant recours à l'application *City Shopy* va être amenée à collecter nombre de données à caractère personnel (nom, prénom, numéro de téléphone, données de géolocalisation, etc.). Sa qualité d'autorité publique la soumet à l'obligation d'engager un DPO.

Les administrations soumises à certaines législations spécifiques[29], telles que les CPAS, sont déjà dotées d'un conseiller en sécurité des données. Néanmoins, cette fonction ne se confond pas avec la fonction de DPO, raison pour laquelle il ne serait pas judicieux de les fusionner dans le chef d'une même personne. En effet, comme nous le verrons, les missions du DPO ne se limitent pas au volet « sécurité » de la protection des données. En outre, le RGPD impose des conditions de qualification et de formation continue propres au DPO.

Le RGPD autorise la mutualisation du DPO, c'est-à-dire qu'un même DPO peut travailler pour plusieurs autorités publiques et/ou organismes publics en même temps. Il faut néanmoins s'assurer que ce DPO sera « facilement joignable »[30] à partir de chaque administration, afin d'assurer son rôle de point de contact pour les personnes concernées, pour l'autorité de contrôle et pour ses collègues. Cela signifie que ses coordonnées (téléphone, mail, lieu de travail) soient communiquées[31].

9. Le rôle du DPO – Le DPO est le chef d'orchestre[32] de la protection des données au sein de l'institution qui l'engage.

Le DPO est un *facilitateur*. Il informe et conseille le responsable de traitement au sujet des règles de protection des données en vigueur. Il aide et sensibilise toute personne impliquée dans les traitements de données effectués par l'administration. Il doit également être le point de contact des citoyens pour les questions relatives à leurs données à caractère personnel, et pour l'autorité de protection des données qui souhaiterait s'informer sur les pratiques menées ou effectuer un contrôle sur celles-ci. Il peut également jouer un rôle essentiel dans la tenue du registre des activités de traitement et l'élaboration des

24. Voir *infra,* point C.
25. Voir *infra,* point A.
26. Voir *infra,* point B.
27. Art. 37.1, a) RGPD.
28. Les notions d'autorité publique et d'organisme public n'ont pas été définies par le RGPD et devront faire l'objet d'une interprétation en droit belge.
29. Art. 24 et 25 de la loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale ; art. 20 à 23 de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral ; art. 10 de la loi du 8 août 1983 organisant un Registre national des personnes physiques.
30. Art. 37.2 RGPD.
31. Groupe de l'article 29, Lignes directrices concernant les délégués à la protection des données, adoptées le 13 décembre 2016 et révisées le 5 avril 2017, WP 243, p. 26 accessible ici : www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf.
32. Selon l'expression de la CNIL. Voir www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees.

analyses d'impact[33], en collectant les informations relatives aux traitements de données, en proposant des conseils, etc.

En l'espèce, un citoyen qui souhaiterait connaître les données collectées à son sujet par l'application *City Shopy* et les faire corriger ou effacer s'adressera au DPO.

Le DPO est également un *contrôleur.* Il vérifie que le RGPD est correctement appliqué au sein de l'institution qui l'engage. En pratique, il doit notamment s'assurer que sont respectés les principes relatifs au traitement de données à caractère personnel[34] et les droits de la personne concernée[35]. À cet égard, le DPO pourrait être amené à devoir dénoncer certaines pratiques au sein de l'administration qui l'engage. C'est ce qui justifie l'importance de lui conférer une réelle indépendance[36].

En l'espèce, le DPO vérifiera que le type et le nombre de données collectées par l'application *City Shopy*, la durée de conservation de celles-ci, la réalité du consentement des citoyens concernés, respectent le RGPD. Il avertira le responsable du traitement de toute illégalité en la matière.

En pratique, le DPO « fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant »[37].

Dans une commune, le DPO pourra utilement se tourner vers le directeur général[38], compte tenu de la mission légale qui est dévolue à ce dernier. En effet, le directeur général est notamment chargé « de la mise sur pied et du suivi du système de contrôle interne du fonctionnement des services communaux (…) [notamment] en ce qui concerne le respect de la législation en vigueur et des procédures »[39]. En outre, il « donne des conseils juridiques et administratifs au conseil communal et au collège communal. Il rappelle, le cas échéant, les règles de droit applicables, mentionne les éléments de fait dont il a connaissance et veille à ce que les mentions prescrites par la loi figurent dans les décisions »[40].

Il est important de souligner que, même si son rôle est essentiel, le DPO n'est pas le responsable du traitement. Si des illégalités sont commises, c'est l'administration responsable du traitement – et son sous-traitant, le cas échéant – qui verront leur responsabilité engagée, et non le DPO[41].

10. Les qualités du DPO – Au vu de ses différentes missions, le DPO doit revêtir de nombreuses qualités, qui le font apparaître comme « un mouton à cinq pattes »[42].

Le RGPD indique que le DPO est « désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 »[43]. Néanmoins, aucun diplôme ou certificat particulier n'est exigé.

L'on peut toutefois déduire des missions du DPO qu'il doit avoir une bonne connaissance de la matière, tant au niveau juridique que de la sécurité informatique. Cette compétence doit être appréciée au regard des types de traitements de données effectués par l'institution qui engage le DPO, de la complexité, de la sensibilité et du volume des données traitées[44]. En outre, il doit faire preuve d'une bonne connaissance de son secteur d'activités, de compétences pédagogiques, de proactivité, de réactivité, de qualités relationnelles dans la gestion d'équipe[45]. Enfin, le DPO doit promouvoir la culture de la protection des données au sein de l'organisme et, à cet égard, faire preuve d'éthique et d'intégrité[46].

11. L'indépendance du DPO – Le DPO doit exercer sa tâche en toute indépendance ce qui signifie qu'il ne peut « recevoir aucune instruction en ce qui concerne l'exercice de ses missions »[47] et qu'il « ne peut être relevé de ses fonctions ou pénalisé par le responsable de traitement ou le sous-traitant pour l'exercice de ses missions »[48]. En outre, le responsable du traitement ou le sous-traitant doivent veiller à ce qu'il n'y ait pas de conflits d'intérêts avec d'autres missions et tâches que le DPO exercerait[49]. En d'autres termes, le DPO

33. Voir *infra.*
34. Art. 5 RGPD.
35. Chapitre III RGPD.
36. Voir *infra.*
37. Art. 38, § 3, RGPD.
38. Secrétaire communal à Bruxelles.
39. L1124-4, § 4, CWADEL.
40. L1124-4, § 5, CWADEL.
41. Groupe de l'article 29, Lignes directrices concernant les délégués à la protection des données, adoptées le 13 décembre 2016 et révisées le 5 avril 2017, WP 243, p. 29 accessible ici : www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf.
42. Selon l'expression de Yasmine Ourari, Juriste à l'eWBS, lors d'un colloque consacré au RGPD, organisé par l'UVCW le 22 novembre 2017 à Wierde.
43. Art. 37.5. RGPD.
44. Groupe de l'article 29, Lignes directrices concernant les délégués à la protection des données, adoptées le 13 décembre 2016 et révisées le 5 avril 2017, *op. cit.*, p. 27.
45. Pour plus de détails, voir art. 37, § 5, RGPD et Groupe de l'article 29, Lignes directrices concernant les délégués à la protection des données, *op. cit.*, p. 27.
46. V. VERBRUGGEN, *op. cit.*, p. 20.
47. Art. 38.3. RGPD.
48. *Idem.*
49. Art. 38.6. RGPD.

ne peut exercer une autre fonction au sein de l'administration, qui l'amènerait à déterminer les finalités et les moyens des traitements de données à caractère personnel[50].

Au sein d'une commune, par exemple, un DPO ne pourrait pas être également directeur général[51].

B. Le registre des activités de traitement (art. 30 RGPD)

12. Le contenu et le rôle du registre – Chaque administration responsable de traitement doit tenir un registre des activités de traitement, qui recense notamment les coordonnées du responsable de traitement, les finalités du traitement, les catégories de personnes dont les données sont enregistrées, les catégories de données enregistrées, le fondement légal du traitement, etc. Si un sous-traitant est impliqué, son registre des activités de traitement ne doit mentionner que les éléments propres à l'activité de sous-traitance, afin d'éviter la tenue de deux registres redondants.

Il s'agit là d'une obligation, assortie d'une exception très limitée qui ne s'appliquera en général pas aux administrations[52].

En l'espèce, la ville qui recourt à l'application « *Shopy City* » devra tenir un registre des activités de traitement indiquant ses coordonnées, les finalités de la collecte des données (promotion du commerce local, promotion du tourisme dans la ville, étude des habitudes de consommation, marketing direct, etc.), les catégories de personnes concernées (les personnes se déplaçant sur le territoire de la ville et ayant téléchargé l'application), les catégories de données enregistrées (nom, prénom, numéro de téléphone, données de géolocalisation), la réalité du consentement[53] des personnes dont les données sont traitées comme fondement légal de ce traitement, etc.

En somme, ce registre est une cartographie des traitements de données. Bien qu'il puisse paraître fastidieux, ce document a du sens. D'une part, lors de sa rédaction, il amène l'administration à se poser les bonnes questions quant à l'utilisation des données des citoyens, ce qui est une manière de la sensibiliser à la matière et de la pousser à vérifier la légalité de ses pratiques. Une fois rédigé, ce registre donne à l'administration une vue d'ensemble des traitements effectués. Cela favorise l'objectif de responsabilisation des acteurs, évoqué plus haut, et facilite le travail de démonstration du respect du RGPD. D'autre part, ce registre favorise également une plus grande transparence des traitements de données effectués, tant à l'égard de l'autorité de protection des données que des personnes concernées.

13. Le lien avec la « future ex » déclaration de traitement – Les réflexes à adopter pour tenir un registre des activités de traitement ne sont, en principe, pas tout à fait inconnus des administrations. Depuis 1998[54], et jusqu'au 25 mai 2018, chaque administration doit déclarer les traitements de données qu'elle met en place à la Commission de la protection de la vie privée. Cette déclaration doit contenir des éléments semblables à ceux qui figureront dans le registre des activités de traitement (coordonnées du responsable de traitement, finalités du traitement, catégories de données, etc.). La CPVP enregistre ensuite la déclaration dans une base de données légalement dénommée le « registre des traitements automatisés de données à caractère personnel ». Ce registre est plus couramment appelé le « registre public », car il est accessible au public, notamment à partir du site internet de la CPVP[55].

Par exemple, le 31 janvier 2017, la ville de Verviers a déclaré à la CPVP recourir à la géolocalisation des véhicules communaux et recueillir à cette occasion des données GPS et GSM[56].

Cette déclaration et le registre public poursuivent plusieurs objectifs.

Pour le citoyen, ce doit être un moyen d'être informé des traitements existants, d'interroger éventuellement le responsable de traitement pour obtenir davantage de renseignements et réagir si des abus sont constatés. De manière plus générale, cela « devrait aussi permettre au public (via le contrôle de la presse par exemple) d'avoir une vue d'ensemble des utilisations de données à caractère personnel en Belgique »[57].

Pour le responsable de traitement, c'est l'occasion de vérifier le respect des conditions légales en la matière[58].

Enfin, pour la CPVP, la déclaration de traitement est une source d'informations par rapport aux traitements

50. Groupe de l'article 29, Lignes directrices concernant les délégués à la protection des données, *op. cit.*, p. 28.
51. Secrétaire communal à Bruxelles.
52. En effet, ce n'est que si l'administration compte moins de 250 employés et qu'elle n'effectue que des traitements de données occasionnels, qu'elle sera dispensée de l'obligation de tenir un registre des activités de traitement (voir art. 30.5 RGPD).
53. Sur cette notion, voir C. de TERWANGNE, K. ROSIER et B. LOSDYCK, *op. cit.*, p. 22.
54. Voir l'article 17 de la loi du 8 décembre 1992, y inséré en 1998.
55. Voir l'onglet « Registre public » sur le site www.privacycommission.be.
56. Cette déclaration est accessible via le registre public, ici https://eloket.privacycommission.be/elg/publicRegister.htm?decArchiveId=135464.
57. Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Chambre, 1990-1990, n° 10610/1, p. 22.
58. Groupe 29, Rapport du groupe de travail « Article 29 » sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne, *op. cit.*, p. 6.

existants. Elle peut ainsi exercer ses missions de contrôle et apprécier la suite à donner aux plaintes éventuelles qui lui sont adressées[59].

Néanmoins, en pratique, ces objectifs ne sont pas atteints. Les consultations du registre public sont très rares, les traitements ne sont pas tous déclarés par les responsables de traitements et la CPVP n'est matériellement pas en mesure de vérifier le contenu de chaque déclaration et d'exécuter les poursuites nécessaires en cas d'abus.

C'est pour ces raisons que le RGPD supprime cette obligation de traitement et la remplace par la tenue d'un registre. Celui-ci est exclusivement interne, mais doit pouvoir être présenté à l'autorité de protection des données à première demande. Cependant, il va de soi que les déclarations de traitement déjà effectuées constituent une bonne source d'information qui pourra utilement nourrir le registre des activités de traitement.

14. Comment faire ? – S'agissant de sa forme, le registre des activités de traitement doit être présenté « sous forme écrite, y compris la forme électronique ». Étant donné qu'il doit pouvoir être communiqué rapidement à l'autorité de protection des données en cas de contrôle des activités de traitement, et que l'administration doit être en mesure d'y retrouver facilement les informations qui y sont logées, notamment si elle est saisie d'une question émanant d'un citoyen, il est conseillé d'utiliser une version numérique plutôt que papier.

Au-delà, il est très utile de prendre connaissance, dès à présent, des bons outils mis à disposition des responsables de traitement par la CPVP. Dans un onglet RGPD – Registre des activités de traitements[60]–, figure un document de synthèse également proposé par la CNIL en France, et reprenant les questions à résoudre pour la constitution dudit registre.

En outre, la CPVP propose un modèle de registre en format Excel[61], qui devrait aider les administrations à être rapidement opérationnelles. Ce modèle contient des onglets par type d'éléments à mentionner. Chacun de ces onglets fait apparaître une liste indicative de propositions pour les types de finalités, de catégories de personnes, de catégories de données, etc., qui pourront utilement inspirer les responsables de traitement.

C. L'analyse d'impact relative à la protection des données (art. 35 RGPD)

15. Le rôle de l'analyse d'impact – cas concret – Une fois rédigé le registre des activités de traitement qui décrit les données utilisées et les traitements effectués, l'administration responsable de traitement doit réaliser une analyse d'impact relative à la protection des données (en anglais, *Data Protection Impact Assessment*). Si un sous-traitant est impliqué, ce dernier peut aider l'administration si nécessaire et sur demande.

L'analyse d'impact est une évaluation des traitements de données mis en place, d'un point de vue juridique et d'un point de vue technique, dans le but d'anticiper les risques en identifiant les mesures techniques et organisationnelles à mettre en place pour éviter au maximum les incidents affectant la sécurité des données[62].

16. Obligation d'effectuer une analyse d'impact dans certains cas – L'analyse d'impact est obligatoire quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées »[63].

Signalons tout d'abord que les termes « *droits et libertés des personnes concernées* » visent le droit à la protection de la vie privée des personnes physiques, mais pas seulement. La protection des données à caractère personnel protège également d'autres droits fondamentaux. Par exemple, en encadrant l'utilisation des données relatives à l'origine ethnique et à la santé, on protège le droit à l'égalité et à la non-discrimination. En limitant l'utilisation des données relatives à l'appartenance syndicale, on protège la liberté d'association. Régler l'usage des données relatives à l'appartenance religieuse encourage la liberté de culte, etc.[64].

En l'espèce, des données relatives à l'origine ethnique, à la santé et à l'appartenance religieuse sont susceptibles d'être collectées par le système de géolocalisation.

59. Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, *op. cit.*, n° 1610/1, p. 22.
60. www.privacycommission.be/fr/registre-des-activites-de-traitement.
61. D'après Valérie Verbruggen, Conseiller juridique à la CPVP, « si ce support pourrait convenir à de relativement petites structures, il ne semble pas adapté à toutes les situations et les responsables de traitement et sous-traitants sont libres d'utiliser d'autres formats (par exemple, un registre « *web based* ») (voir V. VERBRUGGEN, *op. cit.*, p. 9).
62. Voir le document de la CNIL, « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données », disponible ici www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-dpia.
63. Cette obligation est assortie d'exceptions très limitées. L'une d'entre elles vise spécifiquement le secteur public mais est subordonnée au respect de plusieurs conditions. Ainsi, en vertu de l'article 35.10, une analyse d'impact n'est pas nécessaire lorsque le traitement est nécessaire au respect d'une obligation légale ou à l'exécution d'une mission de service public à condition qu'il ait une base juridique dans le droit de l'UE ou en droit belge, que ce droit réglemente cette opération de traitement, qu'une analyse d'impact ait déjà été réalisée à l'occasion de l'adoption de cette base juridique.
64. Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in État de droit et virtualité,* K. BENYEKHLEF et P. TRUDEL (éd), Montréal, Thémis, 2009, p. 210 ; E. DEGRAVE, *E-gouvernement et protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n° 64.

Ensuite, la question se pose de savoir ce qu'est un « *risque élevé* ». Le cas d'espèce en présente-t-il ? Plusieurs sources peuvent être consultées, qui précisent cette notion.

Premièrement, l'article 35.3 du RGPD dresse une liste de traitements de données présentant en eux-mêmes des risques élevés. Il s'agit notamment de « la surveillance systématique à grande échelle d'une zone accessible au public »[65]. Répond, par exemple, à cette hypothèse, un système de vidéo intelligente qui surveille les comportements routiers en isolant chaque véhicule pour identifier sa plaque d'immatriculation[66].

En l'espèce, géolocaliser les citoyens faisant leurs achats consiste en une surveillance systématique à grande échelle d'une zone accessible au public.

Deuxièmement, les autorités de protection de données nationales doivent dresser une liste des types d'opérations pour lesquelles une analyse d'impact est requise[67]. C'est ce qu'a fait la Commission de la protection de la vie privée belge[68]. Elle affirme, par exemple, qu'une analyse d'impact est requise lorsque le traitement vise à enregistrer les connaissances, les prestations, les aptitudes ou l'état de santé mentale d'élèves et à assurer le suivi de l'évolution de ceux-ci, notamment à l'aide de systèmes de suivi des élèves, que ces élèves soient dans l'enseignement primaire, secondaire, tertiaire ou universitaire.

Signalons que, pour éclairer au mieux les responsables de traitements, la CPVP a également dressé une liste de traitements pour lesquels une telle analyse n'est pas requise[69].

Par exemple, l'administration ne doit pas faire d'analyse d'impact s'agissant de l'« enregistrement de visiteurs dans le cadre d'un contrôle d'accès lorsque les données traitées restent limitées au nom et à l'adresse professionnelle du visiteur, à l'identification de son employeur, à l'identification du véhicule du visiteur, au nom, à la section et à la fonction de la personne visitée et au moment de la visite et où les données à caractère personnel traitées peuvent exclusivement être utilisées pour le contrôle d'accès et ne pas être conservées plus longtemps que le temps nécessaire à cette finalité »[70].

Une analyse d'impact ne doit pas non plus être effectuée pour « les traitements de données à caractère personnel effectués par des établissements d'enseignement (…) »[71].

Autres exemples encore, l'analyse d'impact n'est pas requise s'agissant du traitement de « données à caractère personnel qui concernent uniquement les données nécessaires à l'administration des salaires »[72] du personnel, ou « des données à caractère personnel qui concernent uniquement l'administration du personnel en service ou actif pour le compte du responsable de traitement »[73].

Troisièmement, lorsque ces sources n'apportent pas de réponse claire, l'administration responsable de traitement doit effectuer une interprétation au cas par cas en s'aidant de l'interprétation donnée par la CPVP à la notion de « susceptible d'engendrer un risque élevé ». Selon la CPVP[74], cette notion renvoie notamment « aux traitements de données dont il est vraisemblable qu'ils puissent avoir des conséquences néfastes considérables pour les libertés et droits fondamentaux des personnes physiques si l'on ne prévoit pas de mesures de protection adéquates ». Une « conséquence considérable » « signifie que, dans le cas où le risque se produirait, la personne concernée serait sensiblement touchée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux ». Et d'ajouter que « c'est par exemple le cas lorsqu'il est vraisemblable que le traitement puisse engendrer les conséquences néfastes qui sont énumérées au considérant (75) du RGPD ». Entre par exemple dans cette hypothèse, le traitement de données relatives à des personnes vulnérables, comme des enfants.

En l'espèce, la géolocalisation des citoyens et la collecte des données sont visées par ce considérant. Il s'agit, en effet, de l'hypothèse dans laquelle « des aspects personnels sont évalués (…), dans le cadre de (…) l'analyse d'éléments concernant les préférences ou centres d'intérêts personnels, la localisation, les déplacements ».

65. Art. 35.3, c).
66. Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est 'susceptible d'engendrer un risque élevé ' aux fins du règlement (UE) 2016/679,* 4 avril 2017, WP248, disponible ici www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf.
67. Art. 35.4 RGPD.
68. Voir CPVP, annexe 2 du projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable soumis à la consultation publique (CO-AR-2016-004), p. 24 disponible ici www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_FR.pdf.
69. *Ibid.*, annexe 3, p. 26.
70. *Ibid.*, annexe 3, p. 27, n° 6.
71. *Ibid.*, annexe 3, p. 27, n° 7.
72. *Ibid.*, annexe 3, p. 26, n° 1.
73. *Ibid.*, annexe 3, p. 26, n° 2.
74. CPVP, projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable soumis à la consultation publique, *op. cit.*, p. 12, n° 30.

17. Contenu de l'analyse d'impact – Ainsi qu'on l'a déjà dit, l'analyse d'impact est une évaluation des traitements de données envisagés, d'un point de vue juridique et d'un point de vue technique, dans le but d'identifier les mesures techniques et organisationnelles à mettre en place pour éviter au maximum les risques portés à la sécurité des données[75]. Elle doit avoir lieu avant la mise en œuvre du traitement.

Du point de vue juridique, il s'agit de vérifier que sont respectées les règles du RGPD relatives à la nécessité et à la proportionnalité du traitement, comme évoqué précédemment.

En l'espèce, il s'agira de s'assurer que seules les données d'identification et de géolocalisation nécessaires en vue du fonctionnement de l'application sont collectées, d'identifier et formuler une finalité claire pour ce traitement, de vérifier que les citoyens ont été informés des données collectées, de leur destination, de la finalité poursuivie, de leur droit de s'opposer au traitement, etc.

Ces exigences juridiques doivent être respectées pour chaque traitement de données mis en place, quelle que soit sa nature.

Du point de vue technique, l'analyse d'impact consiste à évaluer les risques d'un traitement de données pour la protection de la vie privée des personnes dont les données sont traitées, dans l'hypothèse où celles-ci seraient divulguées suite à une faille de sécurité (accès non autorisé, vol de données, …). L'objectif de cette analyse est de déterminer les mesures à mettre en place, au niveau organisationnel et au niveau technique, pour protéger les données des citoyens.

18. Comment faire[76] ? – Idéalement, la partie juridique de l'étude d'impact aura déjà été réalisée à l'occasion de la rédaction du registre des activités de traitement.

S'agissant de la partie technique de l'analyse, chaque risque sur les droits et libertés des personnes concernées doit être pris en compte. Il s'agit plus précisément d'analyser la vraisemblance qu'un risque se produise et la gravité de l'impact sur les droits et libertés des citoyens si ce risque se produit.

En l'espèce, il y a lieu de vérifier la vraisemblance d'un risque en identifiant notamment les mesures de sécurité qui s'appliquent au serveur enregistrant les données des citoyens. Sont-elles assez efficaces pour contrer un vol de données ? Quant à la gravité de la survenance d'un risque, les données collectées reprenant notamment l'adresse et la géolocalisation des personnes concernées, on doit craindre un risque de cambriolage notamment.

Une fois ces risques identifiés, il y a lieu de décider des mesures techniques et organisationnelles à mettre en place pour réduire le risque à un niveau acceptable. Si cela ne semble pas possible, l'autorité de protection des données doit être consultée[77].

Pour aider les responsables de traitement, la CNIL propose, depuis le 22 novembre 2017, un logiciel spécialement dédié à l'élaboration de l'analyse d'impact ainsi qu'un tutoriel vidéo accessible sur le site internet de la CNIL et sur YouTube. À n'en pas douter, cet outil sera une aide très utile pour les responsables de traitement[78].

Conclusion

L'entrée en application prochaine du RGPD incite les administrations à se plonger dans la protection des données à caractère personnel et à repenser certaines pratiques en la matière. Elle pousse aussi à faire le point sur les acteurs clés de ce régime juridique et les outils nouveaux à mettre en place. Tout ceci dans le but d'aider les administrations à répondre aux enjeux de transparence et de responsabilisation, qui fondent le RGPD.

À certains égards, le RGPD provoquera donc des évolutions positives dans le secteur public. Nous n'assisterons pas à un chamboulement révolutionnaire qui perturberait l'exécution des missions de service public. Nombre de règles sont déjà applicables depuis la loi du 8 décembre 1992 et la directive 95/46 qui ont longtemps régi la protection des données à caractère personnel. Le RGPD constitue ainsi une utile piqûre de rappel à maints égards. Par conséquent, on peut raisonnablement penser que les agents de l'administration seront désormais pleinement sensibilisés à la matière et au fait que la vie privée ne se réduit pas à des règles fastidieuses dénuées de sens. Ce droit fondamental est un enjeu pour la relation de confiance entre le citoyen et l'administration, et pour le fonctionnement de la société démocratique dans son ensemble. Par ailleurs, le RGPD allège aussi certaines pratiques, en supprimant par exemple la déclaration de traitements dont les objectifs de transparence à l'égard des CPVP et d'information des citoyens n'étaient pas atteints, si bien qu'elle était perçue comme une simple formalité administrative ennuyeuse.

75. Voir le document de la CNIL, « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données », disponible ici www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-dpia.
76. Pour plus de détails, voir la méthode proposée par la CNIL, accessible ici : www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf ainsi que les informations proposées par la CPVP, accessibles ici : www.privacycommission.be/fr/analyse-dimpact-relative-a-la-protection-des-donnees.
77. Art. 36 RGPD ; V. VERBRUGGEN, *op. cit.*, p. 15.
78. Le logiciel et le tutoriel sont accessibles ici : www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

Néanmoins, certaines obligations nouvelles provoquent la crainte de coûts importants, en temps et en argent. On songe à l'engagement des DPO. On vise aussi la tenue du registre d'activités de traitement et la rédaction d'une analyse d'impact, qui risquent d'augmenter l'aspect bureaucratique de la protection des données. On ne peut pas non plus ignorer qu'à la faveur d'une meilleure connaissance de leurs droits, les citoyens sollicitent davantage l'administration pour prendre connaissance des données détenues à leur sujet, les faire corriger, s'opposer à leur utilisation, etc.

Ces inconvénients se feront probablement sentir dans les premières années de l'entrée en application du RGPD, le temps de mettre en place et de pérenniser les outils et les pratiques. Ensuite, progressivement, on peut espérer que ces obligations, si elles sont bien concrétisées, contribuent à créer une culture de la protection des données ainsi que des habitudes et des réflexes dans cette matière au sein des administrations.

Une question substantielle demeure toutefois : comment assurer l'effectivité de ces règles pour que les efforts demandés aux administrations ne restent pas sans effet ? Ainsi qu'on l'a dit, nombre de ces règles existent depuis 1992. Pourquoi, jusqu'ici, ont-elles été si peu comprises et appliquées par beaucoup d'administrations ? La même question se pose à l'égard des citoyens. La loi du 8 décembre 1992 organisait déjà des droits d'accès, d'opposition, de correction, et des voies de recours. Pourquoi ces droits et ces recours ont-ils été si peu concrétisés ?

La matière est complexe et le restera. Elle génère, on l'a dit, des charges nouvelles pour les administrations.

À notre sens, deux pistes doivent retenir l'attention, à l'occasion de l'entrée en application du RGPD.

D'une part, les législateurs et les gouvernements doivent saisir l'importance et l'urgence de mettre en place des outils qui permettent à l'administration et au citoyen de traiter les questions de protection des données sans que le citoyen soit découragé par les démarches à accomplir et que l'administration soit confrontée à une augmentation de charge bureaucratique disproportionnée. En d'autres termes, il est urgent de mettre en place un portail internet, qui permettrait au citoyen d'accéder à ses données, de visualiser les échanges de celles-ci au sein de l'administration, de les corriger le cas échéant, sans qu'il faille obliger un agent de l'administration à répondre à ce type de demande individuellement. À cet égard, l'outil mis en place par le Registre national depuis une dizaine d'années déjà, qui permet au citoyen de voir quelles sont ses données enregistrées au Registre national et qui y a eu accès, tout en pouvant générer électroniquement des documents administratifs, gagnerait à être affiné et généralisé[79].

D'autre part, la Commission de la protection de la vie privée sera prochainement remplacée par l'Autorité de protection des données. Gageons du fait que le rôle de cette dernière ne se réduira pas à celui d'un « superflic » chargé de poursuivre les administrations en brandissant la menace d'amendes. La société civile a besoin d'être éclairée par une autorité de protection des données qui soit aussi un organe de la conscience sociale. Une autorité composée d'experts qui l'aide à décider de sa destinée dans l'univers numérique. La société civile a également besoin d'une autorité portée par des personnalités fortes, qui affirment de manière visible un discours lucide et indépendant, visant à accompagner les citoyens confrontés à des technologies dont les enjeux leur échappent. Une autorité, qui, enfin, aide les citoyens et les institutions publiques, notamment, à comprendre pleinement le sens de ces règles et la manière de les appliquer, notamment en créant des outils pédagogiques, simples et concrets, pour faire respecter ces droits en pratique avec la rapidité et l'efficacité que ce respect mérite.

79. Voir www.ibz.rrn.fgov.be/fr/registre-national/mon-dossier/.