RGPD et pouvoirs publics

Degrave, Elise

Published in:
Le RGPD, une arme contentieuse

Publication date:
2024

Document Version
le PDF de l'éditeur

RGPD et pouvoirs publics : de nouveaux arguments pour le contentieux objectif et judiciaire

Elise Degrave

Professeure à la Faculté de droit de l'UNamur
Directrice de l'équipe de recherches en e-Gouvernement du Namur Digital Institute/Crids
Co-directrice de la Chaire Egov de l'UNamur

Introduction

La carte d'identité électronique dans notre portefeuille, un code QR en guise de ticket de train, le versement automatique d'une prime sur notre compte en banque, tous ces éléments en attestent : le numérique imprègne désormais le secteur public dans son ensemble.

Ces outils de tous les jours fonctionnent grâce à de multiples traitements de données à caractère personnel. Il s'agit de données que nous confions à l'État, durant notre vie entière, et qui touchent à toutes les facettes de notre quotidien : santé, famille, emploi, loisirs, etc. En principe, l'État utilise ces données pour nous octroyer des avantages et vérifier que nous respectons nos obligations. Toutefois, techniquement, ces données sur lesquelles nous avons peu de contrôle une fois confiées à l'État pourraient être utilisées de manière plus inquiétante. En Hongrie, par exemple, le gouvernement a décidé de faire pression sur chaque mauvais payeur d'impôts en publiant sur un site web, accessible à tous, leur identité, leur adresse et le montant d'impôts restant dû, pratiquant là un « name and shame » à la chinoise[1]. Doit-on craindre que ce type d'utilisation de nos données apparaisse un jour en Belgique, à la faveur d'un gouvernement illibéral par exemple ? La question mérite d'être posée afin de construire ensemble, grâce au droit, les barrages à de telles pratiques. C'est dire si la protection des données dans le secteur public revêt une importance fondamentale pour maintenir la confiance du citoyen en l'État à l'ère du numérique et protéger les droits humains de chacune et de chacun[2].

1 Cette pratique a conduit à la condamnation de la Hongrie par la Cour européenne des droits de l'homme. Voy. Cour eur. D.H. (gde ch.), arrêt *L.B. c. Hongrie*, 9 mars 2023.

2 À ce sujet en général, voy. E. Degrave, *L'État numérique et les droits humains*, coll. Académie en poche, Bruxelles, Académie Royale, 2024 et le « teasing » vidéo ici : https ://www.youtube.com/watch?v=_RttQqsroek.

Préambule

La structure et le fonctionnement des pouvoirs publics à l'ère du numérique

1. « Front office » et « Back office ». Les outils comme la carte d'identité électronique et les pratiques comme l'automatisation de certains droits se déploient dans le « front office » de l'administration, c'est-à-dire dans la relation entre le citoyen et les pouvoirs publics. Aujourd'hui, cette relation passe de plus en plus souvent par un écran ou une application web.

Quand tout fonctionne bien sur le plan technique, nombre de démarches administratives peuvent désormais être effectuées en quelques clics depuis un ordinateur ou un smartphone, épargnant tant aux citoyens qu'aux administrations les files d'attente aux guichets, de nombreux courriers d'échange d'informations, le risque d'erreurs dans le recopiage des informations, etc.

Si de tels outils et pratiques ont pu être mis en place, c'est parce que, dans les coulisses de l'administration, appelées le « back office », de profonds changements structurels ont été réalisés, qui ont conduit à la mise en place d'une administration « en réseaux », guidée par l'objectif de « collecte unique » des données[3].

2. L'objectif de la collecte unique des données. Depuis son démarrage dans les années 1990, la numérisation de l'administration poursuit un objectif fort : celui de la collecte unique des données. Il s'agit de ne demander qu'une seule fois aux citoyens les informations qui les concernent, à la différence de ce qui se faisait jadis, lorsqu'il fallait communiquer quinze fois son changement d'adresse, par exemple. Aujourd'hui, dès que le citoyen a communiqué une information à une administration, les autres administrations ne peuvent plus la lui réclamer à nouveau.

L'objectif de collecte unique des données et la nécessaire réutilisation de celles-ci entre les administrations ne sont pas que des vœux pieux. Ces impératifs sont consacrés par plusieurs textes normatifs, notamment une loi du 5 mai 2014 qui soumet l'ensemble des SPF fédéraux à l'obligation de collecte unique de données[4].

C'est pourquoi, la structure et le fonctionnement de l'administration sont aujourd'hui organisés dans l'idée de rendre possibles la collecte unique des données et la réutilisation des informations entre les administrations[5].

---

3 À ce sujet, voy. E. Degrave, « Justice sociale et services publics numériques : pour le droit d'utiliser – ou non – internet », *Revue belge de droit constitutionnel*, 2023, pp. 211 à 244.

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

5 Il convient bien évidemment de repenser la structure et le fonctionnement de l'administration également au regard des règles de protection de la vie privée et des données à caractère personnel, ce qui est expliqué dans la suite de cette étude.

3. De l'administration en silos à l'administration en réseaux. À l'époque de « l'administration-papier », les autorités publiques fonctionnaient en « silos », indépendamment les unes des autres. Elles collectaient chacune les informations dont elles avaient besoin. 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 et réclamer éventuellement des précisions, mais aussi pour le citoyen qui était contraint de communiquer de multiples fois la même information aux institutions gérant un dossier à son sujet, d'effectuer des démarches administratives qui impliquaient d'identifier l'administration compétente, de se déplacer, de respecter des horaires stricts et de prendre patience dans les files d'attente.

Avec le numérique, on constate que les administrations peuvent désormais collaborer efficacement en s'échangeant les informations sur les citoyens. La volonté naît alors d'encourager les « synergies entre les divers services et niveaux des pouvoirs publics »[6], dans le but de simplifier les démarches et procédures administratives. La technologie rend aisé et rapide l'échange des informations relatives aux citoyens. Cela permet notamment d'alléger les tâches administratives des citoyens en automatisant l'octroi de certaines allocations, par exemple, et de renforcer l'efficacité de l'administration en améliorant la lutte contre la fraude, notamment[7].

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

Le modèle d'administration en réseaux a devancé, en l'incarnant avant l'heure, la concrétisation du concept de « privacy by design », l'un des principes importants du RGPD[8], qui veut que l'on tienne compte de la protection de la vie privée dès l'étape de conception de l'outil. C'est exactement ce souci de protection de la vie privée dans l'architecture même du modèle d'administration qui a présidé au choix d'organiser l'administration en réseaux.

4. La description du modèle de l'administration en réseaux. En pratique, comment ce modèle se concrétise-t-il ?

---

6 Commission de la protection de la vie privée (ci-après « CPVP »), avis n° 41/2008 du 17 décembre 2008 relatif à une demande d'avis concernant l'avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de services fédéral, n° 5.

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

8 Article 25 RGPD.

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 et placées chacune sous la responsabilité d'une administration sont appelées « sources authentiques de données ». L'idée est de faire en sorte que chaque information relative au citoyen ne soit enregistrée qu'une seule fois par une seule administration du réseau, qui est ensuite responsable de la fiabilité de ces données.

Enfin, on place au cœur de ce réseau d'administrations un outil d'un type nouveau : l'intégrateur de services, dit aussi « 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.

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

Historiquement, le premier réseau du genre est le réseau de la sécurité sociale, qui regroupe les institutions de sécurité sociale et au sein duquel œuvre la Banque-carrefour de la sécurité sociale. Ce réseau et cet intégrateur de services sont en place depuis le début des années 1990[9].

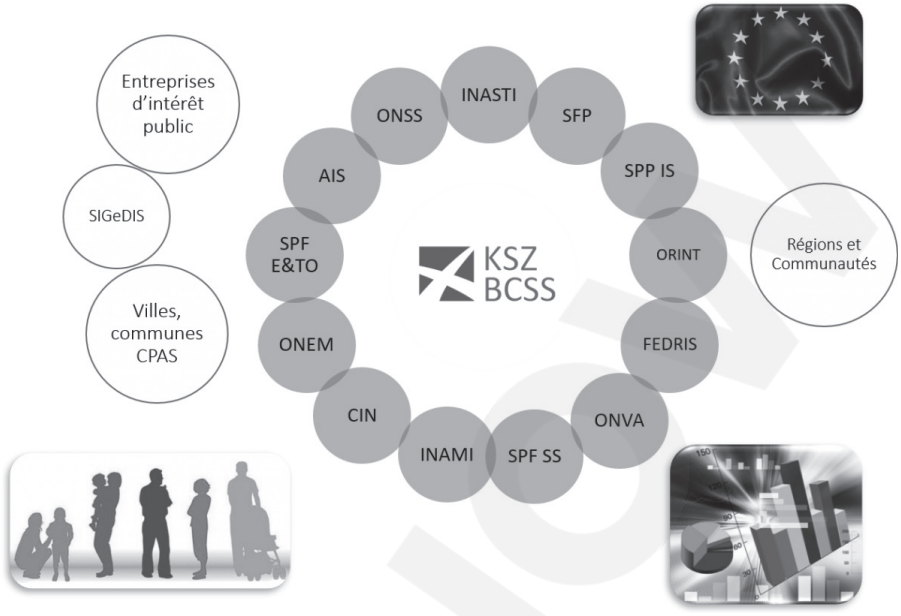
Depuis lors sont apparus d'autres réseaux, tels que le réseau sectoriel de la santé, au sein duquel la plate-forme *eHealth* assume le rôle d'intégrateur de services[10] ou le réseau des véhicules avec en son cœur la Banque-carrefour des véhicules[11].

9 Voy. la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990. Ci-après « loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale ».

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

11 Loi du 19 mai 2010 portant sur la création de la Banque-Carrefour des Véhicules, *M.B.*, 28 juin 2010.

Exemple d'intégrateur de services : la Banque-carrefour de la sécurité sociale (« BCSS »), placée au cœur du réseau de la sécurité sociale[12]



L'administration en réseaux présente de nombreux avantages, mais elle crée aussi des difficultés, s'agissant notamment du respect des exigences du RGPD.

À cet égard, dans cette étude, nous nous concentrons sur les exigences juridiques que le RGPD impose, d'une part, au législateur dans la rédaction des normes qui encadrent les traitements de données à caractère personnel (section 1) et, d'autre part, aux institutions publiques qui effectuent des traitements de données à caractère personnel (section 2). Vu l'ampleur du sujet, nous nous concentrons sur les règles cardinales en la matière, celles qui ont vocation à être le plus souvent mobilisées dans le contentieux objectif et judiciaire[13].

Pour chacune de ces règles, le principe théorique est expliqué et ensuite illustré par un ou plusieurs cas de jurisprudence.

12 https://www.ksz-bcss.fgov.be/fr/a-propos-de-la-bcss/structure-du-reseau.

13 Pour de plus amples détails, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier, 2014.

Section 1

Des arguments applicables à la rédaction des normes encadrant les traitements de données à caractère personnel

5. L'exigence constitutionnelle de légalité. Lorsque l'État collecte, enregistre et/ou réutilise les données des citoyens, il effectue des traitements de données à caractère personnel. Ces traitements de données constituent des ingérences dans le droit fondamental à la protection de la vie privée, comme l'a affirmé à plusieurs reprises la Cour européenne des droits de l'homme, notamment[14].

Dès lors, ces traitements de données sont soumis au respect de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, selon lesquels de telles ingérences sont admissibles à la condition d'être organisées par « une loi » qui doit mentionner certains éléments déterminés. C'est l'exigence de légalité, de laquelle plusieurs arguments peuvent être invoqués pour conduire à l'annulation des normes qui ne respecteraient pas cet impératif.

6. Deux piliers. La légalité est un pilier fondamental de l'État de droit. Elle est garantie par l'article 105 de la Constitution, en vertu duquel l'action administrative doit être encadrée par une loi au sens formel du terme. C'est l'exigence de légalité formelle.

Puisqu'il implique des traitements de données à caractère personnel, l'e-gouvernement est également soumis à l'article 22 de la Constitution qui protège la vie privée des citoyens. Cette disposition constitutionnelle impose au législateur des obligations de légalité substantielle lorsqu'il organise un traitement de données à caractère personnel.

§ 1. Le principe

7. La légalité formelle. S'agissant de la légalité formelle, l'article 22 de la Constitution exige que chaque ingérence dans la vie privée des citoyens soit organisée par une loi au sens formel du terme, c'est-à-dire, une loi, un décret ou une ordonnance bruxelloise.

La Cour constitutionnelle l'a d'ailleurs déjà rappelé à plusieurs reprises, affirmant que « bien que, en utilisant le mot "loi", l'article 8.2 de la Convention européenne [des droits de l'homme] n'exige pas que l'ingérence qu'il permet soit prévue par une "loi", au sens formel du terme, le même mot "loi" utilisé

[14] Voy. not. Cour eur. D.H., arrêt *Amann c. Suisse,* 16 février 2000, req. n° 27798/95, § 65 ; Cour eur. D.H., arrêt *Rotaru c. Roumanie,* 4 mai 2000, req. n° 28341/95, § 43 ; Cour eur. D.H., arrêt *Shimovolos c. Russia,* 21 juin 2011, req. n° 30194/09, §§ 69 et 70.

à l'article 22 de la Constitution désigne une disposition législative »[15]. En effet, « en réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au respect de la vie privée et familiale, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans ce droit ne pourra avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue »[16].

8. La légalité matérielle. La seule existence d'une loi ne peut suffire pour encadrer les traitements de données de citoyens. Encore faut-il que cette loi soit de qualité suffisante pour permettre à chacun de déterminer, clairement et précisément, ce qu'il va advenir des données collectées à son sujet.

La Cour constitutionnelle rappelle d'ailleurs régulièrement que l'article 22 de la Constitution « garantit à tout citoyen qu'il ne pourra être porté atteinte au respect de sa vie privée qu'en vertu d'une disposition législative, et dans les conditions que celle-ci prévoit, de manière à ce que chacun puisse savoir à tout moment à quelles conditions et dans quelles circonstances les autorités publiques pourraient s'ingérer dans ce droit »[17]. Dans le même sens, la Cour européenne des droits de l'homme insiste sur le caractère compréhensible et prévisible de la loi, en soutenant que la loi doit être « énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant, au besoin, de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable, les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé »[18].

S'inspirant de la jurisprudence de la Cour européenne des droits de l'homme[19], la Cour constitutionnelle et la section législation du Conseil d'État ont dégagé les « éléments essentiels du traitement »[20], c'est-à-dire les éléments que le législateur doit déterminer dans la loi organisant le traitement de données envisagé[21]. Cette jurisprudence a d'ailleurs été rappelée maintes fois par l'Autorité de protection des données[22].

---

15 C.C., 18 octobre 2006, n° 151/2006, B.5.6. Voy. égal. C.C., 18 mars 2010, n° 29/2010, p. 19, B.10.2. ; C.C., 21 décembre 2004, n° 202/2004, B.4.3.

16 Voy. not. C.C., 22 septembre 2022, n° 110/2022, B.37.1.

17 C.C., 21 décembre 2004, n° 202/2004, B.4.3. Voy. égal. C.C., 16 mai 2013, n° 66/2013, B.11.1.

18 Voy. not. Cour eur. D.H., arrêt *Sunday Times c. Royaume-Uni*, 26 avril 1979, req. n° 6538/74 ; arrêt *Malone c. Royaume-Uni*, 2 août 1984, § 67 ; arrêt *Amann c. Suisse*, 16 février 2000, req. n° 27798/95, §§ 75 et 76 et arrêt *Leander c. Suède*, 26 mars 1987, req. n° 9248/81, § 50.

19 Cour eur D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95, § 57, *R.T.D.H.*, 2001, pp. 137 et s., note O. De Schutter. Cet arrêt est fondamental en la matière car, pour la première fois, la Cour y dégage les éléments des traitements de données qui doivent figurer dans la loi pour que celle-ci soit précise et prévisible.

20 Voy. not. C.C., 21 décembre 2004, n° 202/2004, B.6.2. et B.6.3. ; C.C., 22 septembre 2022, n° 110/2022, B.11.2. ; C.C., 1er juin 2023, n° 84/2023, B.16.9.

21 Voy. E. Degrave, *L.e-gouvernement et la protection de la vie privée (...)*, n° 103 et références citées.

22 Voy. not. APD, avis n° 36/2020 du 29 avril 2020 sur une demande d'avis concernant un avant-projet d'arrêté royal portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 (CO-A-2020-042), nos 38 et s. ; APD, avis n° 42/2020

Pour définir les « éléments essentiels » du traitement, les hautes juridictions se réfèrent au RGPD et à la directive 95/46 qui l'a précédé. Ces normes, spécifiquement adoptées pour réguler les traitements de données à caractère personnel, permettent ainsi de préciser l'exigence constitutionnelle de légalité et de la rendre applicable à l'univers numérique. On constate que le RGPD forme, avec l'article 22 de la Constitution et l'article 8 de la CEDH, un « tout indissociable » qui émane de la méthode selon laquelle, lorsqu'une disposition conventionnelle trouve écho dans une ou plusieurs dispositions constitutionnelles, « les garanties consacrées par cette disposition conventionnelle constituent un ensemble indissociable avec les garanties inscrites dans les dispositions constitutionnelles en cause […]. Lorsqu'est alléguée la violation d'une disposition du titre II, la Cour tient compte, dans son examen, des dispositions de droit international qui garantissent des droits ou libertés analogues »[23]. « On est, de la sorte, dans une logique, non plus de hiérarchie, mais de circularité. Dans une perspective, non plus de concurrence, mais de complémentarité »[24].

Ainsi donc, pour chaque traitement de données, le législateur doit déterminer lui-même quelle institution a accès à quelles données, pour quoi faire et pendant combien de temps. La détermination de ces éléments doit être l'occasion d'effectuer l'examen de proportionnalité des traitements de données par rapport à l'objectif poursuivi, en évaluant la pertinence et la nécessité des mesures envisagées.

Plus précisément, le législateur doit définir lui-même les *données* utilisées et leur *mode de collecte*.

L'*objectif* poursuivi par le traitement, appelé également « finalité » du traitement, est un élément essentiel de celui-ci.

Par ailleurs, le législateur doit mentionner les *personnes autorisées* à consulter une base de données ainsi que les *conditions* de cette consultation.

---

du 25 mai 2020 sur une demande d'avis concernant une proposition de loi portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 (CO-A-2020-048), nos 16 et s. ; avis no 233/2022 du 29 septembre 2022 sur un avant-projet de loi portant des mesures de police administrative en matière de restrictions de voyage et de Formulaire de Localisation du Passage, nos 6 et s.

23 C.C., 22 juillet 2004, no 136/2004, B.5.3. et B.5.4. Voy. également P. Vanden Heede et G. Goedertier, « De doorwerking van het internationale recht in the rechtsprrak van het Arbitragehof », *in* J. Wouters et D. Van Eeckhoutte (dir.), *Doorwerking van international recht in de Belgische rechtsorde. Recente ontwikkelingen in de rechtsakoverschrijdend perspectief*, Anvers, Intersentia, 2006, pp. 239 à 294 ; J. Velaers, « De samenloop van grondrechten in het Belgische rechtsbestel », *in* A. Nieuwenhuis, L. Dragstra, J. Velaers, L. Huybrechts, H. Wolswijk, F. Salomons, B. de Groot et S. Voet (dir.), *Samenloop van grondrechten in verschillende rechtsstelsels*, Den Haag, Boom Juridische uitgevers, 2008, pp. 81 à 141 ; H. Dumont et C. Hoorevoets, « L'interprétation des droits constitutionnels », *in* M. Verdussen et N. Bonbled (dir.), *Les droits fondamentaux en Belgique*, *op. cit.*, pp. 192 à 198.

24 M. Verdussen, « Introduction », *in La vie privée au travail*, Louvain-la-Neuve, Anthemis, 2011, p. 14.

Il en va de même de la *durée de conservation* des données. Cela suppose que le législateur fixe au moins les délais maximums de conservation des données[25].

Enfin, la *communication* des informations, dite aussi « réutilisation », doit également être organisée par le législateur lui-même[26].

9. La raison d'être de l'exigence de légalité. Si une loi claire, précise et prévisible est nécessaire pour encadrer les traitements de données à caractère personnel, c'est parce qu'il est primordial que les représentants du peuple qui siègent au Parlement mènent un débat démocratique sur ces questions.

Ce débat démocratique doit être *éclairé*. Les questions sont souvent techniques, abstraites. Les auditions au Parlement, notamment, permettent d'interroger publiquement des experts sur les enjeux de cette matière. S'en suivent des débats axés sur les éléments essentiels des traitements de données envisagés. S'agissant, par exemple, de la vaccination contre le Covid-19, un tel débat, s'il avait été mené à l'époque, aurait pu amener à réfléchir à plusieurs questions importantes. Quelles sont les finalités exactes poursuivies par la base de données de vaccination ? Est-il proportionné, au regard de ces finalités, d'enregistrer ces données pendant 30 ans après la date de vaccination ? Quelles autorités auront accès à ces données et pour quoi faire ?

Mener un débat sur ces questions afin de bien encadrer l'utilisation des données à caractère personnel est d'autant plus important que la vie privée est le socle des autres libertés. Par exemple, si les données santé sont mal utilisées, cela portera atteinte à la vie privée mais également au droit à l'égalité et à la non-discrimination, au droit d'aller et venir, à la liberté de culte[27], etc. Protéger la vie privée, c'est protéger l'ensemble des libertés[28].

Ce débat doit également être *éclairant*. Grâce, notamment, aux médias qui le relaient, il est l'occasion d'informer le public sur les questions en jeu, la difficulté d'organiser la balance entre l'efficacité de l'État, d'une part, et la protection des libertés, d'autre part. Pour reprendre l'exemple précité de la vaccination, en expliquant le raisonnement suivi pour encadrer la vaccination, le public pourrait comprendre pourquoi il était nécessaire, le cas échéant,

25 Avis L 37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc.*, Ch., 2004-2005, nos 1598/1 et 1599/1.

26 Voy. not. avis L. 42.064 du 24 janvier 2007 sur un avant-projet de loi « relatif à certains traitements de données à caractère personnel par le Service Public Fédéral Finances », *Doc.*, Ch., no 52-3064/1.

27 Dans l'hypothèse, par exemple, où les données de traçage récolées au moment de la crise du Covid-19 révèlent la fréquentation d'un lieu de culte précis.

28 En ce sens, voy. not. Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in* K. Benyekhlef et P. Trudel (éds.), *État de droit et virtualité*, Montréal, Thémis, 2009, p. 210.

d'enregistrer longtemps des données de vaccination et à quoi cela peut servir. Ce type d'explication permet de gagner la confiance des citoyens à propos de la gestion de leurs données mais également de la vaccination elle-même.

En d'autres termes, à condition de respecter l'exigence de légalité formelle et matérielle, le régime juridique de la protection des données n'empêche pas que des données soient utilisées par l'État, même à des fins de contrôle des citoyens, à condition que cette utilisation soit encadrée par une loi, au terme d'un débat ayant permis, notamment, de faire l'examen de proportionnalité des traitements de données envisagés et de déterminer clairement les éléments essentiels de ces derniers.

§ 2. Illustration jurisprudentielle

10. Le Comité de sécurité de l'information (« CSI »). Le CSI[29] est une autorité composée de deux chambres, l'une compétente pour autoriser la communication des données de sécurité sociale et de santé détenues par l'État (chambre « sécurité sociale et de santé » du CSI)[30] et l'autre pour autoriser certains échanges de données émanant des autorités publiques fédérales (chambre « autorité fédérale » du CSI)[31]. Dans les lignes qui suivent, nous nous concentrons sur la chambre « sécurité sociale et santé » qui fait l'objet d'une intéressante jurisprudence récente.

Aux termes de l'article 39 de la loi du 5 septembre 2018 (« loi CSI ») qui modifie l'article 46 de la loi du 15 janvier 1990 (« loi BCSS »), la chambre « sécurité sociale et santé » est compétente pour déterminer, seule, quelles autorités sont habilitées à (ré)utiliser quelles données et pourquoi[32]. Par exemple, comme l'affirme la loi précitée, le CSI peut, notamment, autoriser la réutilisation, pour des finalités indéterminées, des données détenues par toute institution de sécurité sociale[33]. On constate ainsi que le CSI est habilité par la loi à définir des éléments qui devraient en principe être définis par le législateur lui-même.

29 Sur la composition et le fonctionnement du CSI, voy. C. De Terwangne et E. Degrave (avec la coll. de A. Delforge et L. Gerard), *Protection des données à caractère personnel en Belgique : manuel de base*, Bruxelles, Politeia, 2019, pp. 174 et s.

30 Le CSI, chambre sécurité sociale et santé, a été créé par la loi du 5 septembre 2018 sur le CSI instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, modifiée par la loi du 23 novembre 2023 concernant des mesures de police administrative en matière de restrictions de voyage et de formulaire de localisation du passager et modifiant diverses dispositions relatives au comité de sécurité de l'information.

31 Cette chambre a été créée très récemment par la loi 13 mai 2024 modifiant la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral.

32 Outre le fait que ces décisions ne sont pas débattues démocratiquement, elles sont difficiles à trouver. Elles sont accessibles ici https://www.ksz-bcss.fgov.be/fr/protection-des-donnees/comite-de-securite-de-linformation-csi. Depuis 2018, 734 décisions ont été adoptées, parmi lesquelles il est impossible de faire une recherche par mots-clés ou par type de décision.

33 Article 18 de la loi du 5 septembre 2018 sur le CSI.

Disons-le d'emblée : le CSI est censé n'être qu'un organe de contrôle technique, chargé de vérifier des aspects techniques, comme le fait que telle donnée est bien anonymisée. Mais la loi qui l'institue est tellement floue qu'il exerce *de facto* une compétence de législateur, compétence trop large au regard de l'exigence constitutionnelle de légalité.

Cette compétence trop large déléguée au CSI a été critiquée à plusieurs reprises par l'APD[34], la section législation du Conseil d'État et, plus récemment, sanctionnée par la Cour constitutionnelle. Nous nous concentrons ici sur les avis de la section législation du Conseil d'État et les arrêts de la Cour constitutionnelle.

11. Le CSI dans les avis de la section législation du Conseil d'État. À plusieurs reprises, la section législation du Conseil d'État (« SLCE ») s'est montrée très critique à l'égard du CSI.

Ainsi, dans l'avis qu'elle a rendu au sujet de l'encadrement de la vaccination contre le Covid[35], et se fondant sur l'avis qu'elle avait rendu quelques mois auparavant au sujet du traçage[36] et sur celui rendu au moment de la création du CSI[37], la SLCE rappelle notamment que « l'attribution d'un pouvoir réglementaire à un organisme public, comme le comité de sécurité de l'information[38], n'est en principe pas conforme aux principes généraux de droit public en ce

34 Voy. not. les avis n° 36/2020 du 29 avril 2020 ; n° 42/2020 du 25 mai 2020 ; n° 64/2020 du 20 juillet 2020 ; n° 24/2021 du 2 mars 2021 ; n° 66/2021 du 6 mai 2021 ; n° 228/2022 du 21 décembre 2022.

35 SLCE, avis n° 68.844 du 18 février 2021 sur un avant-projet de loi « portant assentiment à l'accord de coopération du [XX XX] 2021 entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement de données relatives aux vaccinations contre la COVID-19 », n° 28.

36 C.E., 15 juillet 2020, avis n° 67.719/VR sur un avant-projet devenu la loi du 9 octobre 2020 « portant assentiment à l'accord de coopération du 25 août 2020 entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspection d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 se fondant sur une base de données auprès de Sciensano », http://www.raadvst-consetat.be/dbx/adviezen/67719.pdf.

37 C.E., 26 avril 2018, n° 63.202/2 sur un avant-projet devenu la loi du 5 septembre 2018 « instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE », *Doc.*, Ch., 2017-2018, n° 54-3185/001, pp. 140 et s.

38 Note 49 de l'avis cité : voy. d'ailleurs à cet égard la critique qu'avait déjà formulée le Conseil d'État en la matière dans son avis n° 63.202/2 du 26 avril 2018 sur un avant-projet devenu la loi du 5 septembre 2018 « instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE », *Doc.*, Ch., 2017-2018, n° 54-3185/001, pp. 140-142.

qu'il est ainsi porté atteinte au principe de l'unité du pouvoir réglementaire et qu'un contrôle parlementaire direct fait défaut.

En outre, les garanties dont est assortie la réglementation classique, telles que celles en matière de publication, de contrôle préventif exercé par le Conseil d'État, section de législation, et de rang précis dans la hiérarchie des normes, sont absentes. Pareilles délégations ne se justifient dès lors que dans la mesure où elles sont très limitées et ont un caractère non politique, en raison de leur portée secondaire ou principalement technique. Les organismes qui doivent appliquer la réglementation concernée doivent être soumis à cet égard tant à un contrôle juridictionnel qu'à un contrôle politique […]. En conclusion, les délégations visées accordées au Comité de sécurité de l'information doivent être transformées en délégations à un accord de coopération d'exécution, à l'instar de l'article 14, § 9, de l'accord de coopération, pour autant du moins qu'il ne règle aucun nouvel élément essentiel du traitement des données à caractère personnel, mais concrétise tout au plus ce qui découle déjà de l'actuel accord de coopération. Si cela ne s'avère pas possible, cet accord de coopération sera d'abord complété[39] ».

Ainsi donc, les avis de la section législation du Conseil d'État soulignent sans détour le manque de contrôle parlementaire, juridictionnel et politique sur le CSI. En outre, les décisions du CSI ne bénéficient pas d'une publicité suffisante, ne sont pas soumises au contrôle préventif de la section législation du Conseil d'État et leur statut n'est pas clair.

12. Le CSI dans les arrêts de la Cour constitutionnelle. Pour la première fois en 2022, la Cour constitutionnelle a également eu l'occasion de se prononcer sur le CSI. Elle s'est prononcée à nouveau, et dans le même sens, en 2023[40]. Emboîtant le pas à la SLCE, la Cour constitutionnelle se montre elle aussi très critique. Son raisonnement, tout à fait en lien avec celui de la SLCE, se déroule en trois temps.

Tout d'abord, la Cour constate que le CSI est doté du pouvoir de prendre des décisions en matière de traitements de données à caractère personnel.

39 Note 50 de l'avis cité : Comparer avec les critères d'évaluation qu'utilise la Cour constitutionnelle pour apprécier les délégations de pouvoir réglementaire par le législateur à une autorité administrative autonome ou à un organisme public décentralisé ; voy. C.C., 11 juin 2015, n° 86/2015, B.22.4, et C.C., 9 juin 2016, n° 89/2016, B.9.6.4 : « Les articles 33, 105 et 108 de la Constitution ne s'opposent pas à ce que, dans une matière technique déterminée, le législateur confie des compétences exécutives spécifiques à une autorité administrative autonome soumise tant au contrôle juridictionnel qu'au contrôle parlementaire et n'interdisent pas au législateur d'accorder des délégations à un organe exécutif, pour autant qu'elles portent sur l'exécution de mesures dont le législateur compétent a déterminé l'objet, en particulier dans les matières techniques et complexes » ; voy. C.C., 19 novembre 2015, n° 162/2015, B.8.4 : « L'article 33 de la Constitution et l'article 20 de la loi spéciale du 8 août 1980 ne s'opposent pas à ce que le législateur confie des compétences exécutives spécifiques à un organisme public décentralisé qui est soumis à une tutelle administrative et à un contrôle juridictionnel ».

40 C.C., 22 septembre 2022, n° 110/2022 et C.C., 1er juin 2023, n° 84/2023.

En effet, « les délibérations du CSI ont une portée contraignante notamment pour les personnes dont le traitement des données personnelles est autorisé par ce Comité »[41]. En l'espèce, il était question de l'accord de coopération du 12 mars 2021 concernant le traitement de données relatives aux vaccinations contre la Covid-19, ayant reçu l'assentiment par loi, décrets et ordonnance des différents législateurs du pays. Cet accord de coopération attribuait au CSI le pouvoir d'autoriser la communication des données de vaccination, notamment aux « personnes et instances chargées d'une mission d'intérêt public »[42], notion particulièrement large.

Ensuite, la Cour, se fondant sur les propos de la SLCE, rappelle qu'un tel pouvoir de décision suppose d'être limité à des considérations techniques ou de n'avoir qu'une portée secondaire[43]. Or, soutient-elle, pour ses délibérations, le pouvoir d'appréciation du CSI n'est pas délimité par la loi. Le CSI est donc doté d'un « pouvoir réglementaire », c'est-à-dire le pouvoir de faire des normes, puisqu'il peut définir lui-même les éléments essentiels du traitement. Par exemple, l'accord de coopération précité délègue au CSI le soin de définir les destinataires des données de vaccination. Pour être conforme à la Constitution, un tel pouvoir réglementaire doit notamment être soumis aux garanties qui s'appliquent à la loi, comme l'a dit également la SLCE : publication, contrôle préventif exercé par la section de législation du Conseil d'État, rang précis dans la hiérarchie des normes, etc.[44] Or, ces garanties ne sont pas respectées par les délibérations du CSI.

Enfin, la Cour en conclut qu'« en habilitant la chambre "sécurité sociale et santé" du Comité de sécurité de l'information, dont le statut n'est pas précisé par la loi ni le pouvoir d'appréciation délimité par celle-ci, à prendre des décisions en matière de traitements des données à caractère personnel qui lient les tiers, sans que de telles décisions puissent être soumises au contrôle parlementaire, l'article 5 de l'accord de coopération du 12 mars 2021 prive les personnes concernées de la garantie d'un tel contrôle, sans que cela soit justifié par une exigence découlant du droit de l'Union européenne »[45].

13. Modification législative. Le tollé provoqué depuis longtemps par le CSI dans la doctrine[46], puis dans la jurisprudence[47] et même les médias[48], a

41 C.C., 22 septembre 2022, n° 110/2022, B.38.2 ; 1er juin 2023, arrêt n° 84/2023, B.30.2.

42 Article 5 dudit accord de coopération du 12 mars 2021.

43 C.C., 1er juin 2023, n° 84/2023, B.31.

44 C.C., 22 septembre 2022, n° 110/2022, B.38.2 ; 1er juin 2023, n° 84/2023, B.31.

45 C.C., 1er juin 2023, n° 84/2023, B.31. Dans le même sens : 22 septembre 2022, n° 110/2022, B.39.

46 Voy. not. C. De Terwangne et E. Degrave (dir.), *La protection des données à caractère personnel en Belgique. Manuel de base*, Bruxelles, Politeia/Crids, 2019, pp. 176 et s. ; E. Degrave, « Traçage, fichage, profilage : la vie privée touchée par le covid », *in* F. Bouhon *et al.* (dir.), *Le droit public belge face à la crise du Covid-19 : quelles leçons pour l'avenir ?*, Bruxelles, Larcier, 2022, pp. 785-805.

47 Voy. not. les arrêts de la Cour constitutionnelle précités.

48 Voy. not. *Le Soir* (Ph. Laloux), « Vie privée : le CSI en (tout) petit comité », 5 mai 2021, accessible ici : https://www.lesoir.be/370434/article/2021-05-05/vie-privee-le-csi-gestionnaire-de-donnees-sante-en-tout-petit-comite.

poussé le législateur à tenter de répondre aux critiques concernant l'attribution d'un pouvoir réglementaire inconstitutionnel au CSI. Ainsi, la loi du 23 novembre 2023[49] modifie l'article 46 de la loi BCSS.

Elle affirme désormais noir sur blanc que les délibérations du CSI sont attaquables devant le Conseil d'État. D'ailleurs, pour la première fois, le 12 juin 2024, le Conseil d'État a annulé une délibération du CSI autorisant la communication à l'ONSS de données de santé par la Banque-carrefour de la sécurité sociale et par le SPF Santé publique[50].

En outre, cette nouvelle loi précise que « les délibérations du [CSI] ont une portée limitée et technique » et qu'elles « décrivent pour une situation déterminée et pendant une période déterminée l'application des éléments essentiels du traitement, qui sont définis dans les bases juridiques visées à l'article 6 du RGPD ». Bien que cette disposition, et notamment la portée du terme « décrivent », soit difficilement compréhensible, on peut raisonnablement penser que le législateur souhaite par-là confirmer que le CSI n'a qu'un rôle technique d'exécution des éléments essentiels du traitement définis dans les normes législatives qui fondent tout traitement de données au sein du service public.

Il n'en demeure pas moins que le caractère contraignant des délibérations du CSI ne semble pas remis en cause, étant donné qu'il s'agit toujours de délibérations et non d'avis. Il s'agit donc de décisions qui lient des tiers, raison d'ailleurs pour laquelle elles sont attaquables devant le Conseil d'État. En outre, jusqu'ici, les normes législatives organisant les traitements de données en matière de sécurité sociale et de santé ont été rédigées en tenant compte du rôle du CSI pour préciser les éléments essentiels de ces traitements, ce rôle étant le sien depuis 2018. Affirmer, dans la loi de 2023, que le CSI n'a soudainement plus qu'un rôle technique ne change rien au fait que les législations en la matière ne sont pas toujours elles-mêmes assez précises puisqu'elles ne définissent pas nécessairement les éléments essentiels de ces traitements que le CSI n'aurait qu'à exécuter.

L'histoire dira donc si, en pratique, le CSI refusera de se prononcer sur l'application de lois trop floues ou si cette modification législative n'est que de la poudre aux yeux qui n'empêchera pas le CSI de continuer à adopter des délibérations contraignantes définissant, de manière inconstitutionnelle, les éléments essentiels des traitements en la matière…

49 Loi du 23 novembre 2023 concernant des mesures de police administrative en matière de restrictions de voyage et de formulaire de localisation du passager et modifiant diverses dispositions relatives au comité de sécurité de l'information.

50 C.E., 12 juin 2024, n° 260.091.

Section 2

Des arguments applicables à l'exécution des traitements de données à caractère personnel au sein du secteur public

14. La collecte unique des données et ses conséquences juridiques. Ainsi qu'on l'a dit d'entrée de jeu, l'objectif phare de l'e-gouvernement en Belgique est celui de la collecte unique des données (« only once »). Pour rappel, il s'agit de permettre aux individus de ne communiquer qu'une seule fois les informations qui les concernent, à charge pour les administrations de se communiquer les informations dont elles ont besoin, sans les réclamer à nouveau aux personnes concernées.

On a vu que cet objectif a généré la mise en place d'une administration en réseaux fondée sur la réutilisation maximale des données par les administrations, dans l'idée de ne pas redemander à la personne concernée une information déjà disponible dans une des bases de données de l'État. Cette réutilisation maximale des données met en lumière l'importance particulière, dans ce contexte, de plusieurs exigences du RGPD. Ces exigences s'appliquent à tout responsable du traitement, qu'il œuvre au sein du secteur public ou du secteur privé. Elles prennent toutefois une coloration particulière dans un contexte de maximisation de la réutilisation des données que les citoyens ont été obligés de fournir à l'État.

Dans les lignes qui suivent, nous mettons en lumière les bases de licéité possibles et l'obligation de collecte indirecte des données (§ 1), l'obligation d'exactitude et de mise à jour des données (§ 2), l'obligation de minimisation des données (§ 3) et le consentement. Pour chacune de ces exigences, nous expliquons le principe théorique et l'illustrons grâce à la jurisprudence.

§ 1. La licéité du traitement et l'obligation de collecte indirecte des données

A. Le principe

15. Les bases de licéité – Article 6 du RGPD. Comme on l'a dit plus haut, une autorité publique n'a d'autres compétences que celles que lui confie la loi. C'est pourquoi, de manière générale, tout traitement de données effectué dans le secteur public doit avoir une base légale.

C'est ce que confirme le RGPD. En se référant à l'article 6 du RGPD, on constate que deux bases de licéité confirment cette exigence de légalité de l'action administrative et peuvent donc justifier un traitement de données par une autorité publique.

Premièrement, l'article 6.1, c), du RGPD autorise tout traitement « nécessaire au respect d'une obligation légale ». Par exemple, enregistrer les données d'identité des citoyens dans les registres de la population est un traitement de données nécessaire pour respecter la loi du 19 juillet 1991 sur les registres de la population.

Deuxièmement, s'inscrivant dans la même ligne, l'article 6.1, e), autorise les autorités publiques à effectuer tout traitement de données « nécessaire à l'exécution d'une mission d'intérêt public » ou « relevant de l'exercice de l'autorité publique ». Par exemple, le fait pour une commune de traiter les données des détenteurs d'un permis d'environnement pour leur envoyer des informations relatives à la législation applicable en la matière correspond à l'exercice d'une mission d'intérêt public[51].

16. L'obligation de collecte indirecte des données. Traiter des données de manière licite, comme l'impose l'article 5.1, a), du RGPD, suppose de respecter l'ensemble des règles de droit applicables. Cela signifie qu'il faut respecter le RGPD, mais également toute autre norme s'appliquant au traitement concerné. À cet égard, dans l'e-gouvernement belge, une obligation spécifique s'impose aux autorités publiques : celle de la collecte indirecte des données, qui est une conséquence de l'objectif de collecte unique des données. Cette obligation est organisée par plusieurs législations[52] qui imposent aux autorités publiques qui y sont soumises de demander les données à l'institution qui en dispose déjà, moyennant le respect de certaines balises. Il leur est donc interdit de redemander ces informations aux personnes qui les ont déjà fournies.

L'obligation de collecte indirecte des données n'est pas qu'un principe symbolique. C'est une véritable obligation juridique qui, si elle n'est pas respectée, peut vicier la décision prise par l'autorité publique concernée. À ce jour, elle est pourtant peu connue des avocats et donc peu mobilisée devant les cours et tribunaux.

B. Illustration jurisprudentielle

17. Données utilisées par un CPAS. Dans un arrêt du 21 avril 2010[53], la cour du travail de Bruxelles fait droit à la demande d'un assuré social, Monsieur E.G., qui réclamait le revenu d'intégration sociale. Le CPAS refusait l'octroi

51 E. Degrave (dir.), *L'ABC du RGPD. Dictionnaire pratique à destination des administrations*, Namur, UVCW, 2018, p. 91.

52 L'obligation de collecte indirecte de données est prévue par différentes législations. Voy. e.a. l'article 6 de la loi du 8 août 1983 organisant un registre national des personnes physiques ; article 8, § 3, de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral ; article 6 de l'ordonnance du 17 juillet 2020 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier.

53 C. trav. Bruxelles (8e ch.), 21 avril 2010, R.G. nos 2008/AB/51591 et 2009/AB/51809.

de cette indemnité, au motif que Monsieur E.G. n'avait pas fourni un certain nombre de documents et avait dès lors manqué à son devoir de collaboration.

Dans sa motivation, la cour du travail rappelle l'existence de l'article 11 de la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale, qui prévoit que « lorsque les données sont disponibles dans le réseau, les institutions de sécurité sociale sont tenues de les demander exclusivement à la Banque-Carrefour ». La cour affirme qu'il faut déduire de cette disposition légale qu'« un manque de collaboration du demandeur ne peut être envisagé à propos d'informations auxquelles le CPAS peut accéder, accessibles via la Banque-Carrefour de la sécurité sociale »[54].

Or, en l'espèce, « la plupart des documents prétendument manquants étaient accessibles via la Banque-Carrefour ou le Registre national : le CPAS n'avait pas à la demander à Monsieur E.G. ; il aurait dû les recueillir d'initiative »[55].

C'est pourquoi, la cour décide que Monsieur E.G. a droit au revenu d'intégration sociale[56].

§ 2. L'obligation d'exactitude et de mise à jour des données

A. Le principe

18. Article 5 du RGPD. Les données traitées par les institutions publiques doivent être exactes et, si nécessaire, tenues à jour, en vertu de l'article 5.1, d), du RGPD. Cette obligation est particulièrement importante dans le contexte de l'e-gouvernement fondé sur la réutilisation maximale des informations. En effet, toute erreur affectant une donnée ayant vocation à être réutilisée aurait un effet domino.

Par application de l'obligation précitée de collecte indirecte des données, les autorités publiques sont tenues de mettre à jour les données qu'elles utilisent, lorsque cette mise à jour est disponible dans le réseau sectoriel auquel elles appartiennent.

B. Illustration jurisprudentielle

19. Données du Registre national. C'est ce qu'a rappelé la cour du travail de Liège, dans un arrêt du 27 juin 2006, faisant application de l'obligation de collecte indirecte en matière de droit à la pension[57]. L'Office national des pensions reprochait à un homme pensionné de ne pas l'avoir averti du décès de son épouse, ce qui avait des conséquences au niveau du montant de la

54 *Ibid.*, 4e feuillet.
55 *Ibid.*, 6e feuillet.
56 *Ibid.*, 8e feuillet.
57 C. trav. Liège, 27 juin 2006, *J.L.M.B.*, 2007, pp. 1043-1047.

pension qui lui était due. L'Office national des pensions exigeait de récupérer les sommes indûment payées depuis cinq ans, en application du délai de prescription applicable en cas de mauvaise foi de l'assuré social ou lorsque l'indu trouve son origine « dans l'abstention du débiteur de produire une déclaration prescrite par une disposition légale ou réglementaire ou résultant d'un engagement souscrit antérieurement », plutôt que de se soumettre au délai de prescription de six mois en principe applicable[58].

Cet assuré social avait averti la commune du décès de son épouse. Cette information était donc enregistrée au Registre national. Faisant partie du réseau sectoriel de la sécurité sociale, l'Office national des pensions y avait donc accès par l'intermédiaire de la Banque-Carrefour de la sécurité sociale.

Compte tenu de ces éléments de fait et de droit, la cour affirme qu'« un assuré social ne peut se voir imposer personnellement une obligation qui doit déjà être légalement remplie par une institution dont c'est la mission. C'est donc à tort que l'ONP soutient que l'information transmise par la Banque-Carrefour doit être doublée par une information émanant de l'assuré social et que seule celle-ci permettrait au pensionné de remplir ses obligations envers lui […] »[59].

§ 3. L'obligation de minimisation des données

A. Le principe

20. Articles 5 et 25 du RGPD. Aux termes de l'article 5.1, c), du RGPD, les données traitées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Il s'agit de l'exigence de « minimisation des données », qui vaut non seulement pour les données collectées pour la première fois mais également pour les données réutilisées.

Pour encourager l'effectivité de cette obligation, l'article 25 du RGPD impose la protection des données dès la conception et par défaut. Par conséquent, l'autorité publique doit mettre en place des « mesures techniques et organisationnelles pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient traitées ». Elle doit veiller en particulier à ce que ces données ne soient pas « rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée ». En effet, il ne faudrait pas que l'ensemble des personnes travaillant au sein d'une autorité publique

58 Ces délais sont imposés par l'article 21, § 3, de la loi du 13 juin 1966 relative à la pension de retraite et de survie des ouvriers, des employés, des marins naviguant sous pavillon belge, des ouvriers mineurs et des assurés libres.

59 C. trav. Liège, 27 juin 2006, *op. cit.*, p. 1047.

aient toutes accès, du seul fait de faire partie de cette autorité, aux bases de données détenues par celles-ci si cela ne se justifie pas pour l'exécution de leurs missions.

B. Illustration jurisprudentielle

21. Redevance parking impayée. Dans la décision de la chambre contentieuse de l'APD du 23 décembre 2020[60], il est question du respect de cette exigence à l'occasion d'une collecte indirecte de données. À l'origine de cette affaire, une automobiliste porte plainte auprès de la chambre contentieuse de l'APD au motif qu'à l'occasion d'un contrôle du stationnement, une société spécialisée en stationnement de rue et un huissier de justice ont commis plusieurs illégalités dans le traitement de ses données à caractère personnel, concernant notamment le non-respect de l'exigence de minimisation des données[61].

La chambre contentieuse fait droit aux arguments de l'automobiliste. Premièrement, les données de l'automobiliste enregistrées dans le registre de la Direction d'Immatriculation des Véhicules (DIV) – notamment sa plaque d'immatriculation et son adresse – ont été consultées de manière prématurée, « avant l'écoulement du délai qui lui était donné pour s'acquitter spontanément du montant de la redevance réclamée ». Alors que l'infraction de stationnement a eu lieu le 2 janvier, les données de l'automobiliste ont en effet été consultées le 3 janvier, ce qu'a confirmé le contrôle réalisé par l'Inspecteur général de l'APD. La chambre contentieuse rappelle d'ailleurs qu'il incombait à la société de stationnement de rue « d'organiser cet accès dans le respect des principes de la protection des données dès la conception et par défaut [article 25 RGPD] de manière à mettre en œuvre le principe de minimisation des données de manière effective »[62].

Quant au formulaire de contact envoyé par l'huissier de justice à la personne concernée pour le suivi de la mise en demeure, la chambre contentieuse constate qu'« aucun astérisque ou autre mention n'indique que la personne concernée est libre de choisir un des modes de communication (numéro de téléphone, numéro de GSM, adresse e-mail) et que certaines données sont donc facultatives. […] La présentation et la formulation utilisées donnent à penser qu'il n'y a pas d'alternative à la collecte de *toutes* les informations au regard de chaque rubrique du tableau ». Elle en conclut à un manquement à l'article 5.1, c), du RGPD dans le chef de l'huissier de justice.

60 APD, chambre contentieuse, Décision quant au fond 81/2020 du 23 décembre 2020. À noter que le 26 mai 2021, la cour des marchés a annulé l'amende imposée à l'huissier de justice au motif – très discutable – qu'une « simple réprimande » suffisait.

61 Sur cette affaire, voy. également E. Degrave, *L'État numérique et les droits humains, op. cit.*, nos 51 et s.

62 APD, *op. cit.*, no 82.

§ 4. Le consentement

A. Le principe

22. Articles 4 et 6 du RGPD. Figurant également parmi les bases de licéité mentionnées à l'article 6 du RGPD, le seul consentement du citoyen est-il suffisant pour justifier légalement que l'autorité publique traite ses données ? Non. L'autorité publique doit toujours pouvoir se prévaloir d'une base légale justifiant le traitement effectué. En effet, le consentement ne peut être une base de licéité du traitement de données qu'à la condition d'être « libre, spécifique, éclairé et univoque », comme précisé à l'article 4, 11), du RGPD. Or, dans la relation entre l'autorité publique et le citoyen, on ne peut considérer que le consentement est « libre » étant donné le caractère déséquilibré de la relation[63], dès lors que le citoyen dépend de l'autorité publique pour l'exécution de ses obligations et l'obtention d'allocations, notamment.

B. Illustration jurisprudentielle

23. EBox. L'eBox est la boîte e-mail officielle proposée à chacun par l'État pour les démarches avec les autorités publiques. À plusieurs reprises[64], l'APD a rappelé qu'aucun citoyen ne peut être contraint d'utiliser un outil numérique pour exercer ses démarches administratives en ligne. Son consentement libre et éclairé est requis. En effet, en l'état actuel de la législation, il n'est pas obligatoire d'utiliser l'eBox. Il existe donc une « liberté de choix concernant l'activation de l'eBox pour personnes physiques »[65]. C'est pourquoi l'article 6 de la « loi eBox » affirme que « les personnes physiques doivent avoir expressément consenti au préalable à l'échange électronique de messages via l'eBox et doivent pouvoir retirer ce consentement à tout moment »[66].

63 Cons. 43 RGPD.

64 CPVP, avis n° 47/2018 du 23 mai 2018 relatif à un avant-projet de loi relative à l'échange électronique de messages avec les instances publiques, n° 14 ; APD, avis n° 154/2019 du 4 septembre 2019 relatif à l'avant-projet de décret modifiant le décret du 27 mars 2014 relatif aux communications par voie électronique entre les usagers et les autorités publiques wallonnes et à l'avant-projet de décret modifiant le décret du 27 mars 2014 relatif, pour les matières visées à l'article 138 de la Constitution, aux communications par voie électronique entre les usagers et les autorités publiques wallonnes, n° 13 ; APD, avis n° 165/2019, concernant un projet d'arrêté royal modifiant les articles 136/1 et 136/2 de l'arrêté royal d'exécution du Code des impôts sur les revenus 1992 relatifs à l'envoi électronique des avertissements-extraits de rôle, n° 9 ; APD, avis n° 169/2022 du 19 juillet 2022 concernant un avant-projet de loi modifiant la loi du 27 février 2019 relative à l'échange électronique de messages par le biais de l'eBox, n° 23 ; APD, avis n° 253/2002 du 1er décembre 2022 concernant une demande d'avis portant sur l'article 31 d'un avant-projet de loi portant des dispositions fiscales diverses, n° 15.

65 APD, avis n° 169/2022 précité, n° 9. À noter que même dans leur activité professionnelle d'indépendant, les personnes physiques peuvent refuser l'eBox. L'utilisation obligatoire de l'eBox, telle qu'envisagée initialement par le législateur, risquerait « d'avoir des effets disproportionnés à l'égard de [ces] personnes […], en particulier celles qui ne disposent pas du matériel et des connaissances nécessaires pour leur permettre de communiquer, de manière aisée, par voie électronique avec les instances publiques » (APD, avis n° 169/2022 précité, n° 23).

66 Article 6 de la loi du 27 février 2019 relative à l'échange électronique de messages par le biais de l'eBox. Dans le même sens, s'agissant de l'usage de l'eBox en Région wallonne, voy. l'article 10 de l'arrêté du

Ce consentement du citoyen est une « garantie appropriée complémentaire »[67], devant respecter certains critères qui, ces derniers temps, n'ont pas toujours été respectés d'après le Médiateur fédéral ayant reçu de nombreuses plaintes à ce sujet[68].

La personne concernée doit donc être informée au préalable des conséquences juridiques de l'échange électronique des messages via l'eBox. Elle doit également pouvoir retirer son consentement à tout moment, y compris à l'égard de certaines instances publiques déterminées[69]. En effet, « les destinataires qui souhaitent recevoir par la poste les communications d'instances publiques déterminées doivent conserver cette liberté de choix, par exemple afin d'être sûrs que les messages n'échappent pas à leur attention ou afin de garantir que tous les membres concernés de la famille reçoivent et puissent suivre les informations »[70]. S'il fallait imposer l'utilisation de l'eBox, cela ne pourrait se faire qu'en vertu d'une obligation légale, conformément à l'article 6 du RGPD[71].

24. Dispositif Microsoft. L'APD a aussi constaté l'illégalité d'un dispositif mis en place par le SPF Finances, consistant à exiger du citoyen qu'il crée un compte chez Microsoft et y encode des données à caractère personnel, pour accéder à l'information fiscale en ligne[72]. Elle a rappelé à cette occasion que les exigences précitées du RGPD, celle de la minimisation des données traitées (article 5 RGPD) et celle d'un consentement valable de la personne concernée (article 6 RGPD), s'appliquent dans la relation avec les entreprises privées. L'APD s'est fondée sur l'article 5 du RGPD pour affirmer que « l'imposition, par des autorités publiques, de l'utilisation d'un compte Microsoft pour accéder à une application qui ne met à disposition que des informations publiques et pas des données à caractère personnel est contraire au RGPD »[73]. Se fondant sur l'article 6 du RGPD, elle

Gouvernement wallon du 12 juin 2014 relatif aux communications par voie électronique et à l'échange électronique de messages par le biais de l'eBox entre les usagers et les autorités publiques wallonnes ; article 4 du décret wallon du 27 mars 2014 relatif aux communications par voie électronique entre les usagers et les autorités publiques wallonnes.

67 APD, avis n° 253/2022 du 1er décembre 2002 portant sur l'article 31 d'un avant-projet de loi portant des dispositions fiscales diverses, n° 15.

68 Médiateur fédéral, *Rapport d'activité 2022*, p. 18.

69 Voy. not. APD, avis n° 169/2022, *op. cit.*, n° 10.

70 APD, avis n° 47/2018, *op. cit.*, n° 17.

71 En vertu du principe de légalité des ingérences dans les droits fondamentaux, en l'occurrence le droit à la protection de la vie privée, une telle obligation légale supposerait notamment que le législateur identifie l'objectif légitime poursuivi et puisse démontrer la proportionnalité du moyen que serait l'exclusivité de la voie numérique pour les contacts avec l'administration. Il devrait donc démontrer que ce moyen est pertinent pour atteindre l'objectif légitime poursuivi, mais également qu'il est nécessaire, c'est-à-dire qu'il ne crée pas, pour les citoyens (tous), de dégâts collatéraux évitables par d'autres moyens, comme les démarches administratives hors ligne.

72 APD, Recommandation n° 01/2019 du 6 février 2019 relative à l'obligation de créer un compte utilisateur chez Microsoft pour consulter des applications de services publics.

73 *Ibid.*, p. 8.

précise qu'« obliger la personne concernée à créer un compte auprès d'un sous-traitant et à accepter la politique en matière de protection de la vie privée de ce sous-traitant invalide le consentement en tant que fondement juridique du traitement »[74]. Notons que depuis cet avis, le SPF Finances a mis fin à ce dispositif[75].

Conclusion

Au travers de ces lignes transparaît l'enrichissement du droit constitutionnel et du droit administratif grâce au RGPD qui, à maints égards, vient se greffer sur les exigences fondatrices de notre État de droit.

S'agissant de l'exigence de *légalité* qui encadre l'action administrative, le RGPD conduit à une plus grande précision des normes qui organisent les traitements de données à caractère personnel dans le secteur public. Comme l'ont mis en évidence tant la Cour européenne des droits de l'homme que la Cour constitutionnelle et le Conseil d'État, le législateur doit désormais déterminer lui-même les « éléments essentiels » des traitements de données effectués dans l'administration. Parmi ceux-ci, la « finalité du traitement », par exemple, doit déterminer explicitement l'objectif poursuivi, au-delà de la simple mention des « missions légales » à accomplir. À ce jour, l'exigence de légalité, dans ses versants de légalité formelle, d'une part, et matérielle, d'autre part, n'est pas encore pleinement respectée en pratique. On le constate notamment au travers de l'importante jurisprudence de la Cour constitutionnelle concernant notamment le Comité de sécurité de l'information, organe de contrôle aux pouvoirs (trop) larges qui n'a pas fini de faire parler de lui. C'est dire l'importance de la mobilisation par les avocates et les avocats de ces arguments pour mettre fin aux normes inconstitutionnelles portant atteinte au droit à la protection de la vie privée, notamment.

L'exigence de *contrôle* de l'action administrative est également affinée grâce au RGPD et est à mettre en lien avec un objectif phare de l'e-gouvernement belge, celui de la collecte unique des données, appelé aussi le principe « only once ». Cet objectif est traduit dans notre ordre juridique par une obligation légale figurant déjà dans plusieurs normes législatives et pourtant trop peu connue jusqu'à présent : l'obligation de collecte indirecte des données. Pour respecter pleinement l'obligation de collecte indirecte des données dans toutes ses facettes, plusieurs impératifs du RGPD revêtent une importance particulière. Cette contribution l'a montré, en théorie et en pratique, à propos

74 *Ibid.*

75 APD, Divulguer des données ne peut pas être une condition pour accéder à l'information fiscale ; https://www.autoriteprotectiondonnees.be/citoyen/divulguer-des-donnees-ne-peut-pas-etre-une-condition-pour-acceder-a-linformation-fiscale.

de la licéité des traitements de données, de l'obligation d'exactitude et de mise à jour de données, de l'obligation de minimisation des données et du recours au consentement. Autant d'impératifs qui renforcent encore davantage le devoir de minutie des administrations. Ce sont également autant d'arguments d'un genre nouveau pour les avocats qui veillent, en pratique, à la légalité des traitements de données et, partant, au respect des droits humains et des piliers de notre État de droit.

Élise DEGRAVE