TABLE DES MATIERES

I. INTRODUCTION

A l'heure actuelle, la circulation des données à caractère personnel constitue un des points majeurs de notre époque. En effet, nous vivons dans une société de plus en plus digitalisée et numérisée, ce qui rend donc la problématique de la circulation des données à caractère personnel de plus en plus importante. Néanmoins, ce phénomène de digitalisation croissante dans la vie quotidienne des individus n'est pas sans danger pour les citoyens.

Lorsqu'on focalise le point de vue sur la relation entre l'administration fiscale et le contribuable, ainsi que nous le verrons, on peut apercevoir que le fisc dispose d'un grand nombre d'informations sur les citoyens par le biais d'un système de circulation des données entre les administrations. Néanmoins, ce système de circulation des données n'est pas sans failles et peut donc porter atteinte de manière disproportionnée au droit à la vie privée des individus. Ceci est d'autant plus pertinent au regard du contexte de crise sanitaire que nous connaissons, étant donné les procédures de traçabilité mises en place par le gouvernement.

Grâce à ce propos introductif, nous avons dressé le portrait de notre contribution qui se concentrera essentiellement sur un thème précis, à savoir l'échange de données entre l'administration fiscale et les autres administrations et la compatibilité de ces échanges avec les normes protectrices de la vie privée et des données à caractère personnel. C'est donc pourquoi nous nous concentrerons sur la thématique de l'échange de données entre l'administration fiscale et les autres administrations. Nous tenterons ensuite d'analyser la problématique des procédés de *datamatching*, *datamining* et de profilage au regard de la protection des données à caractère personnel et de la vie privée.

La présente contribution se structurera en trois parties. La première consistera à esquisser les contours du droit de la protection des données à caractère personnel en Belgique. La seconde partie se concentra principalement sur la problématique des échanges de données entre le SPF Finances et les autres administrations, ainsi que leur compatibilité avec le droit à la vie privée et le droit de la protection des données à caractère personnel sous différents aspects. La troisième partie consistera à illustrer et à exposer les enjeux et les dangers de l'utilisation et de la réutilisation de données, au travers de l'actualité.

II. PARTIE 1 : LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN BELGIQUE : PRÉSENTATION SOMMAIRE

1) Propos introductifs

Sans prétendre à l'exhaustivité, nous allons tenter de dresser un portrait global et sommaire de la protection des données à caractère personnel au sein de l'Etat belge. Le présent propos se contentera de dresser une présentation globale du RGPD ainsi que les dispositions législatives belges pertinentes permettant d'appréhender la problématique des échanges de données à caractère personnel entre le SPF Finances et les autres administrations.

2) Le RGPD[1]

Depuis son adoption, le RGPD constitue la pierre angulaire du droit de la protection des données à caractère personnel au sein des Etats membres de l'Union européenne. Dans ce chapitre, nous nous contenterons de présenter le RGPD dans son contexte actuel. Nous proposons donc de présenter les motifs liés à l'adoption du règlement et ses principaux objectifs et sa structure. Nous analyserons ses impacts sur les échanges de données à caractère personnel dans le cadre de la deuxième partie.

a. Les motifs liés à l'adoption du RGPD et ses objectifs

Le RGPD, instrument législatif européen, est le fruit d'une longue négociation de quatre années à l'échelon européen. En réalité, le RGPD est venu abroger la directive 95/46[2] qui constituait alors la base européenne d'harmonisation des droits nationaux en matière de protection des données à caractère personnel. Etant donné l'absence d'effet direct de la directive, il existait un certain nombre de disparités entre les différents droits étatiques des membres de l'Union européenne. Ce constat a donc conduit les négociateurs européens à choisir la voie d'un règlement afin d'uniformiser au maximum le droit de la protection des données personnelles à l'échelon européen tout en déléguant certains aspects aux Etats membres[3]. Nous

[1] 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 (règlement général sur la protection des données

[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOUE*, L.281, 23 novembre 1995, pp.31-50.

[3] V. VERBRUGGEN, « Titre 1: RGPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne », in *Le Règlement général sur la protection des données (RGPD/GDPR)*, p.27.

pouvons trouver une trace de ce constat au considérant n°13 du RGPD. Le RGPD a permis de clarifier la portée de certains droits dont bénéficient les personnes concernées par les traitements de données et, d'autre part, il est venu renforcer le rôle des autorités de contrôle[4].

Le RGPD a pour but de renforcer le contrôle et la transparence sur les diverses manipulations qui peuvent être opérées sur les données personnelles. Pour atteindre cet objectif, le législateur de l'Union a opéré sur deux fronts. D'un côté, il est venu imposer plusieurs obligations qui reposent, notamment sur les entreprises et sur les entités publiques, en ce compris les autorités fiscales. De l'autre côté, il est venu clarifier et préciser les différentes compétences dont disposaient les autorités nationales de contrôle du respect de la vie privée afin de faire respecter de manière effective les différentes obligations (NDLR : en Belgique, nous avions la Commission pour la Protection de la Vie Privée qui fut supprimée et remplacée par l'Autorité de protection des données depuis le 25 mai 2018, suite à l'adoption de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données[5]).

Notons que, bien qu'il opère une réforme allant dans le sens d'une protection accrue des droits des personnes concernées par un traitement de données à caractère personnel, le RGPD ne fait pas pour autant l'unanimité en matière fiscale.

b. La structure du RGPD

Le RGPD ne demeure pas moins un instrument législatif complexe comprenant 99 articles et 173 considérants. Néanmoins, nous pouvons synthétiquement regrouper les dispositions du RGPD en trois corps de règles :

- Les principes relatifs au traitement des données à caractère personnel et les droits des personnes concernées.
- La responsabilisation croissante des acteurs pour le traitement des données à caractère personnel (Principe *d'accountability)*.
- Les divers outils et les diverses clés accordés aux différents acteurs permettant d'accroître l'effectivité de la réglementation[6].

---

[4] S. DE RAEDT, "The impact of GDPR on Belgian Tax Authorities", R.D.T.I, 2017/1-2, p. 130-131.
[5] *M.B.*, 10 janvier 2018, E.V. 25 mai 2018
[6] K. JANSSENS et M. NUYTTEN, "De Algemene Verordering Persoonsgegevens: van theorie naar praktijk", *R.D.C-T.D.H*, 2018/5, p.402.

c. Critique du RGPD

Bien que le RGPD opère une réforme allant vers une plus grande protection des droits des personnes concernées par des traitements de données à caractère personnel, certains auteurs critiquent le critiquent dans son applicabilité en matière fiscale. Par exemple, le RGPD prévoit la possibilité de restreindre certains droits, dont le droit d'accès aux données à caractère personnel ainsi que le droit à l'information, conformément à l'article 23.1 e)[7].

Certains auteurs estiment que le législateur accorde, de manière parfois anticonstitutionnelle, un régime de faveur par rapport au régime applicable aux entités privées. Cette différence de traitement pose d'autant plus question dans la mesure où le SPF Finances collecte et conserve des données sans le consentement des personnes concernées. Il dispose en outre de pouvoirs considérables[8], comme par exemple le profilage dans un datawarehouse[9].

Compte tenu de ces affirmations, T. AFSCHRIFT cite les exemples de la dispense de donner des informations au contribuable dans le cas où cela nuirait à l'enquête ou bien lorsque des informations sont collectées chez des tiers. Cet auteur estime que, au final, les principes protecteurs du RGPD sont applicables sauf lorsque les informations sont utiles au contribuable[10].

d. Cadre législatif belge

La protection des données à caractère personnel en Belgique est régie par plusieurs instruments législatifs. Dans un premier temps, il convient de souligner l'impact du RGPD, pierre angulaire du droit de la protection des données à caractère personnel. Au niveau belge, le Règlement européen a induit l'adoption rapide de quatre lois importantes :

- La loi du 3 décembre 2017 consacrée à l'Autorité de Protection des données remplaçante de la Commission de la protection de la vie privée[11].

---

[7] Pour un exposé détaillé des droits des personnes concernées voy. O. TAMBOU, « Droits des personnes concnernées » in *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, p.169-248.
[8] T. AFSCHRIFT, « GDPR: Un système à la mesure du fisc ! », *Sem. Fisc.* 2018/37, n°351, p.1. disponible sur https://www.idefisc.be/view-article.php?idefisc_numero_id=201809
[9] Sur les notions de datamining et datawarehouse, voy. Chapitre IV.
[10] T. AFSCHRIFT, *op. cit.*.
[11] *M.B.*, 10 janvier 2018., p.989.

- La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[12] (ci-après LTD) qui précise les éléments du RGPD pour lesquels les législateurs nationaux ont une marge de manœuvre.
- Loi du 5 septembre 2018 instituant le comité de sécurité de l'information[13] (ci-après loi CSI).
- Loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre national et les registres de population, opérant une réforme importante quant à la loi sur le Registre national[14].

Ces différentes lois ont définitivement abrogé l'ancien système mis en place 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[15] (ci-après Loi « Vie privée »).

Les traitements de données à caractère personnel au sein du SPF Finances, dans le cadre de ses missions, sont réglementés par la loi du 3 août 2012[16] telle que modifiées par les lois précitées dans laquelle le législateur régit les traitements de données à caractère personnel du SPF Finances dans le cadre de ses missions.

Certains auteurs regrettent l'adoption trop rapide de ces lois dans une problématique importante, non seulement pour la vie privée des contribuables, pour ce qui nous préoccupe, mais aussi pour celle des citoyens en général. En effet, certains auteurs estiment que la qualité des lois fait défaut en raison de la rapidité à laquelle elles ont été adoptées[17].

---

[12] *M.B*, 5 septembre 2018, p.68616.
[13] Loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre 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, *M.B.* 10 septembre 2018, p.69589.
[14] *M.B.* 13 décembre 2018, p. 98465.
[15] *M.B.*, 18 mars 1993, pp.5801-5814.
[16] Loi du 3 août 2012 portant des dispositions relatives aux traitements de données à caractère personnel réalisés par le Service Public fédéral Finances dans le cadre de ses missions, *M.B.* 24 août 2012, p. 50670.
[17] C. DE TERWANGNE, E. DEGRAVE, A. DELFORGE et L. GERARD, *La protection des données à caractère personnel en Belgique : manuel de base*, 2019, Bruxelles, Politeia, p.24.

III. PARTIE 2. LES ÉCHANGES DE DONNÉES À CARACTÈRE PERSONNEL ENTRE LES ADMINISTRATIONS

1) Propos introductif

Les échanges de données entre administrations doivent être replacés dans leur contexte. En effet, en raison du développement technologique et numérique, les administrations, dont le SPF Finances, ont dû adapter leurs méthodes de fonctionnement et de travail afin de traiter de manière efficace les éléments d'informations dans le cadre de leurs missions. A cet effet, la méthode de fonctionnement des administrations a progressivement changé de cap, allant d'un fonctionnement cloisonné de chaque administration vers une méthode de collecte unique. Cette ouverture progressive entre administrations poursuit deux objectifs. D'une part, simplifier la tâche de l'administration qui n'a plus besoin de traiter et collecter individuellement les données à caractère personnel et, d'autre part, simplifier la tâche du citoyen qui ne communique ses données qu'une seule fois. A cet effet, le législateur belge avait déjà adopté en 2012 la mise en œuvre d'un « intégrateur de services » qui sert de point de transit et de point de contact au niveau des sources authentiques de données[18].

Les échanges de données à caractère personnel entre administrations consistent en des échanges de données opérés sur base d'une collaboration entre les différentes administrations de l'Etat belge. En pratique, un transfert de données relatives aux revenus pourrait avoir lieu entre le SPF Sécurité Sociale et le SPF Finances, ce dernier voulant connaître la situation familiale d'un contribuable, par exemple. Cette matière a également fait l'objet de certains aménagements suite à l'adoption du RGPD.

2) La situation avant le RGPD

a. L'autorisation préalable des Comités sectoriels

Avant l'entrée en vigueur du RGPD en date du 25 mai 2018, les échanges internes de données à caractère personnel entre autorités publiques était balisé par la mise en place de comités sectoriels auxquels il fallait demander une autorisation. Ces comités sectoriels faisaient partie de l'organisation interne de l'ancienne CPVP (Commission pour la Protection

[18] M. KNOCKAERT, « La loi du 30 juillet 2018 : l'échange de données à caractère personnel dans le secteur public », *R.D.T.I,* 2019/1, n°74, p7.

de la Vie Privée). Concrètement, les différentes administrations étaient les gardiennes de ce que l'on dénomme « des sources authentiques de données ». Ces sources authentiques de données consistent en des bases de données dont les administrations sont les responsables en termes de vérification d'exactitude, de mise à jour et de sécurité[19].

Lorsqu'une entité devait consulter une de ces bases de données, elle devait demander une autorisation au Comité sectoriel compétent. A cet effet et conformément à l'ancien article 36bis de la loi « Vie privée », le Comité sectoriel compétent pour le SPF Finances était le Comité sectoriel Autorité Fédérale. Celui-ci disposait de la compétence d'autorisation relative à l'accès aux sources authentiques de données détenues par un Service Public Fédéral ou un organisme public doté de la personnalité juridique dépendant de l'autorité fédérale. Ce Comité Sectoriel était donc compétent pour les autorisations d'accès aux données contenues dans les sources authentiques gérées par le SPF Finances. Le Comité Sectoriel pour l'Autorité Fédérale disposait donc d'un certain pouvoir, dans la mesure où il pouvait refuser l'accès aux données à caractère personnel contenues dans les bases de données du SPF Finances.

Dans un arrêt[20] concernant la loi du 14 juin 2017 modifiant l'article 36bis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[21], la Cour constitutionnelle a eu l'occasion de mettre en exergue l'importance que comportait le droit à la vie privée prévu à l'article 22 de la Constitution ainsi que l'article 8 de la CEDH dans le cadre du traitement de données à caractère personnel[22]. A cet égard, la CEDH a également jugé que les traitements de données à caractère personnel sont considérés comme des ingérences dans le droit à la vie privée tel que prévu par l'article 8 de la CEDH[23]. L'interprétation donnée par la CEDH et la Cour constitutionnelle sont d'autant plus pertinentes lorsque le citoyen est dans une relation avec l'administration. En effet, le SPF Finances, détient un certain nombre de données à caractère personnel obtenues sans le

---

[19] E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* coll. CRIDS, Bruxelles, Larcier, 2014, n°12 et s.
[20] C.Const., arrêt n°153/2018, 8 novembre 2018.
[21] *M.B.*, 28 juillet 2017.
[22] Arrêt précité, cons. B.8.4.
[23] C.E.D.H, *Rotaru c. Roumanie*, 4 mai 2000, req. 28341/85, §57. Voy. not. C.E.D.H, 26 mars 1987, *Leander c. Suède*, §§ 47-48; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 66-68; 17 décembre 2009, *B.B. c. France*, § 57; 10 février 2011, *Dimitrov-Kazakov c. Bulgarie*, §§ 29-31; 18 octobre 2011, *Khelili c. Suisse*, §§ 55-57; 9 octobre 2012, *Alkaya c. Turquie*, § 29; 18 avril 2013, M.K. c. France, § 26; 18 septembre 2014, *Brunet c. France*, § 31.

consentement de la personne concernée. Dans la relation qui nous préoccupe, le contribuable est obligé de communiquer une grande partie de ses données à caractère personnel s'il ne veut pas être en contravention à la loi. En effet, l'article 315 du Code d'impôts sur les revenus[24] prévoit l'obligation pour les contribuables de rentrer leur déclaration sous peine de subir une sanction conformément à l'article 444 CIR/92. En ayant égard aux enseignements donnés par la CEDH et la Cour constitutionnelle, les règles en matière de traitements de données à caractère personnel doivent donc respecter les exigences de légalité, nécessité et proportionnalité.

Concernant spécifiquement la condition de légalité, cette dernière doit être respectée au regard de deux aspects : la légalité formelle et la prévisibilité. La condition de légalité formelle, induit que les règles doivent être fixées par le législateur fédéral ou fédéré en fonction de la répartition des compétences. La condition de prévisibilité contient l'obligation de prévoir une règle suffisamment claire et précise pour les personnes concernées[25].

De manière synthétique, en ce qui concerne la situation avant la mise en œuvre du RGPD, nous pouvons constater une forme de contrôle opérée par les Comités sectoriels. Malgré les critiques opérées par la doctrine concernant les garanties d'indépendance et d'impartialité, les Comités sectoriels avaient le mérite d'opérer comme des gardiens de terrain de la vie privée des citoyens en général[26].

A titre d'exemple, nous pouvons voir une illustration du contrôle du Comité Sectoriel pour l'Autorité fédérale dans le contexte des échanges automatiques de renseignement sur les comptes financiers. Ainsi, l'ancien Comité sectoriel de la Commission de la vie privée avait critiqué le système de reporting[27] dans son ensemble. Le Comité a estimé que les obligations relatives aux données à caractère personnel contenues dans le MCAA[28] ne sont pas suffisantes par rapport aux garanties offertes non seulement par le RGPD mais également par

[24] Ci-après CIR/92.
[25] C. Const., arrêt n°2/2021 du 14 janvier 2021, cons. B.19.2.
[26] E. DEGRAVE, « Protection des données et Comités sectoriels : avant et après le RGPD », *R.D.T.I,* 2018/4, n°73, p.96.
[27] CRS = Common Reporting Standard
[28] « Multilateral Competent Authority Agreement » acronyme anglais de OCDE, N*orme d'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale*, Paris, Éditions OCDE, 2014, http://dx.doi.org/10.1787/9789264222090-fr.

la « Loi vie privée »[29] et l'ancienne directive 95/46[30]. Le Comité a spécifiquement jugé que les dispositions de la section 5 du MCAA, concernant les fuites de données, ne coïncident pas avec les obligations de notification à l'Autorité de protection des données (art 33 RGPD) et aux obligations de notification à la personne concernée (art 34 RGPD)[31].

b. Les motifs de suppression des Comités sectoriels

Etant donné l'étendue des pouvoirs des comités sectoriels, il fallait instituer un contrôle des différentes décisions ce qui ne semble pas forcément avoir été le cas. En effet, le système mis en place par le législateur avant le RGPD paraissait déjà critiquable au niveau de l'indépendance, de l'impartialité, et de l'absence de voies de recours contre les décisions des comités sectoriels[32].

Le législateur avait mis en exergue trois motifs qui justifiaient, selon lui, la suppression des comités sectoriels[33].

Dans un premier temps, le législateur estimait que le cadre légal dans lequel opéraient les Comités Sectoriels était imprécis voire lacunaire, en ce sens qu'ils n'avaient pas une compétence bien délimitée et demeurait silencieux pour ce qui est des procédures pour lui soumettre des autorisations.

Ensuite, le législateur fit remarquer que faire ressortir les Comités sectoriels de la Commission de la vie privée (ancienne C.P.V.P) rendait impossible un contrôle de légalité de leurs décisions. En effet, d'une part, rendre compétent la C.P.V.P pour contrôler la décision rendait sa position inconfortable puisqu'elle devait contrôler des décisions de ses propres organes et, d'autre part, il demeurait un flou concernant la nature juridique des décisions prises par les Comités sectoriels. Cette incertitude rendait, à tout le moins, hasardeuse la possibilité

---

[29]Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B* 18 mars 1993, aujourd'hui abrogée remplacer par la loi du 30 juillet 2018.

[30] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, aujourd'hui remplacée par le RGPD.

[31] Comité sectoriel pour l'Autorité fédérale, Délibération AF n°39/2017 du 14 décembre 2017, pp.5-8.

[32] Cf. infra ; Pour un exposé détaillé voy. E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, coll. Crids, Bruxelles, Larcier, 2014, n°492 et s.

[33] Projet de loi portant création de l'Autorité de protection des données, Rapport fait au nom de la Commission de la justice par M. Egbert Lachaert, *Doc. parl* ., Ch. repr., sess. ord. 2017-2018, n 2648/6, pp. 6-7.

d'un recours devant le conseil d'Etat. En raison de cet état du droit, le droit belge contrevenait à l'article 28 §3 de la directive 95/46[34].

3) L'impact du RGPD sur les échanges de données : le système des protocoles

Aux termes de l'article 109 de la loi de 2017 portant création de l'autorité de protection des données et supprimant la Commission pour la vie privée, les comités sectoriels ont été supprimés au profit d'un système de protocoles mis en place par l'article 20 de la loi du 30 juillet 2018. L'article 20 prévoit que, lorsqu'un transfert de données à caractère personnel doit être opéré entre deux administrations, ces dernières doivent conclure un protocole de transfert sauf exceptions prévues par la loi.

Le protocole consiste en un document écrit qui doit être rédigé lorsqu'une autorité fédérale doit opérer une communication de données à caractère personnel. Cette dernière doit être effectuée pour réaliser une mission légale ou l'exercice de l'autorité publique[35]. A cet égard, le SPF Finances a conclu plusieurs protocoles, récemment, dans le cadre de la crise du coronavirus[36].

Le système des protocoles mis en place par la loi du 30 juillet 2018 semblait toutefois poser certains problèmes.

---

[34] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 23 novembre 1995, *JOUE*, pp.31-50 ; L. GERARD, « Le comité de sécurité de l'information : illustration d'une incohérence législative », *R.D.T.I.*, 2018/4, n° 73, p57. ; voy. également E. DEGRAVE, « La Commission de la protection de la vie privée : un organisme invincible ? », obs . sous Cour administrative du GrandDuché du Luxembourg, 12 juillet 2005, *R.D.T.I.*, 2006, pp . 225-241

[35] L. GERARD, « Le comité de sécurité de l'information : illustration d'une incohérence législative », *R.D.T.I.*, 2018/4, n° 73, p56.

[36] *Protocole d'encadrement de traitement de données au sens de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, entre le Service Public Fédéral Finances et le Service Public de Wallonie Economie, emploi, recherche concernant l'utilisation de données TVA en vue de l'octroi d'indemnités compensatoires dans le cadre des mesures contre le coronavirus COVID-19* disponible sur https://finances.belgium.be/fr/sur_le_spf/vie-priv%C3%A9e/%C3%A9changes-de-donn%C3%A9es-externes ; *Protocole d'encadrement de traitement de données au sens de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, entre le Service Public Fédéral Finances et le Service Public régional de Bruxelles – Bruxelles Economie et Emploi concernant l'utilisation de données TVA en vue de l'octroi d'une aide aux entreprises exerçant des activités non-essentielles dans le cadre de la crise sanitaire du Covid-19*, disponible sur https://finances.belgium.be/fr/sur_le_spf/vie-priv%C3%A9e/%C3%A9changes-de-donn%C3%A9es-externes

a. Les problèmes liés à la suppression des Comités sectoriels

Initialement, le législateur n'avait pas prévu de contrôle remplaçant celui opéré par les Comités sectoriels. Par conséquent, les échanges de données prévus par les protocoles sont potentiellement en proie à des dangers.

Un des problèmes pointés par la doctrine est le fait que la loi ne prévoyait pas des exigences de mentions dans les protocoles. Ceci induit que les administrations étaient libres d'entériner le contenu qu'elles veulent dans les protocoles. A cet effet, le Conseil d'Etat n'a pas manqué de faire remarquer qu'utiliser le verbe « pouvoir » dans la loi renvoie à une appréciation libre de la part des autorités publiques, ce qui entraînerait une insécurité juridique et une entrave au principe constitutionnel de légalité[37]. Les exigences de loyauté et transparence prévues dans le RGPD prohibent le caractère opaque des traitements de données dans le cadre de transferts de données entre organismes publics. Ce principe a notamment été illustré dans l'arrêt *Smaranda Bara*[38] de la CJUE.

En vue de répondre à l'absence de contrôle reprochée à l'ancien système, l'article 35/1 § 2 de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral[39] prévoit désormais la possibilité d'un contrôle par l'Autorité de protection des données sur les délibérations émises par le Comité de sécurité de l'information, que nous étudierons *infra*.

b. Le rôle du DPO et le contrôle interne du protocole

Pour ce qui est du contrôle opéré sur les échanges de données, l'article 20 de la loi du 30 juillet 2018 prévoit de demander l'avis du délégué à la protection des données (DPO[40]). Le RGPD avait enjoint les administrations, fiscales y compris, de mettre en place un DPO, conformément à l'article 37 du Règlement. Ce type de fonction n'était pas inconnue par

---

[37] M. KNOCKAERT, *op. cit.* p.10. voy. Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, M.B., 5 septembre 2018, p. 21, « (…) le règlement de cette question par l'avant-projet ne satisfait pas à l'exigence de légalité dès lors, d'une part, que le protocole n'est pas rendu obligatoire alors qu'il devrait l'être et que, d'autre part, l'avant-projet n'énonce pas, de manière suffisamment précise, les différents éléments sur lesquels doivent porter ces protocoles »

[38] C.J.U.E. (3e ch.), 1er octobre 2015, *Smaranda Bara*, C-201/14, pour un exposé détaillé de l'affaire voy. M. KNOCKAERT, *op. cit.*, p.13.

[39] *M.B*, 29 août 2012, p. 53170.

[40] *Data Protection officer*

le SPF Finances car, déjà en 2012, la loi avait organisé la mise en place d'un service de sécurité de l'information et de protection de la vie privée (SSIPV) au sein du SPF Finances (ci-après Service Privacy et Security). A l'heure actuelle, le DPO n'est autre que le chef de ce service.

De manière générale, le DPO a pour fonctions principales de faire respecter les principes et les règles émanant du RGPD au sein de l'entité publique ou privée dans laquelle il opère, selon le cas. Il va également servir de point de contact entre les entités responsables de traitement et les personnes concernées par un ou plusieurs traitements de données à caractère personnel[41]. En ce qui concerne les autorités publiques, dont le SPF Finances, il est obligatoire de mettre en place un DPO, conformément à l'article 37.1.a) du RGPD.

Pour pouvoir mener à bien ses missions, le DPO doit être indépendant tant au niveau hiérarchique que fonctionnel, conformément à l'article 39 du RGPD[42].

Au sein du SPF Finances, le rôle du DPO sera de contrôler tout projet d'échange de données avec une autre autorité publique à l'aide du Service Privacy et Security, tel que le prévoient l'article 20 de la LTD et l'article 8 de la loi du 3 août 2012.

c. Le Service Privacy et Security

Suite à une opinion déjà favorable de l'ancienne C.P.V.P[43], le législateur a mis en place le Service de Sécurité de l'Information et la Protection de la Vie Privée (SSIPVP) aux termes de l'article 8 de la loi du 3 août 2012[44]. Le fonctionnement de ce service a été quelque peu modifié à la suite de l'adoption de la loi du 5 septembre 2018 en son article 74. En effet, comme nous l'avons analysé supra, le DPO est désormais à la tête de ce service qui l'assiste dans le cadre de ses missions. Cet organe, dépendant directement du président du comité de

[41] M. KNOCKAERT, *op. cit.*, p.20.
[42] Pour plus de détails sur le rôle du DPO, voy. A. BEELEN, « Fiche de guidance n°11 : le délégué à la protection des données », in *Guide pratique du RGPD*, Bruylant, Bruxelles, pp.83-91.
[43] Voy. C.P.V.P, Recommandation n°2/2012 du 8 février 2012 relative aux principes de bases à respecter lors de traitements de données à caractère personnel impliquant le SPF Finances, p.8, n°11. ; C.P.V.P, avis n°11/2012 du 11 avril 2012 relatif à l'avant-projet de loi relatif aux traitements de données à caractère personnel réalisés par le Service Public Fédéral Finances dans le cadre de ses missions, p.9, n°29.
[44] Libellé comme suit : *« Il est créé au sein du Service public fédéral Finances, un Service de Sécurité de l'Information et de Protection de la Vie Privée qui est placé sous l'autorité directe du président du Comité de direction du Service public Fédéral Finances.*
Ce service assiste le Délégué à la protection des données dans l'exercice de ses missions prévues dans le 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 ainsi que dans les dispositions prises en exécution de ce Règlement ».

direction est appelé Service *« Privacy et Security »* au sein du SPF Finances. Celui-ci a plusieurs missions :

- Il est le point de contact entre le SPF Finances et l'Autorité de Protection des données
- Il soutient les projets mis en place par le SPF Finances en termes de protection de la vie privée et protection des données.
- Il apporte un soutien technique à l'initiative législative en matière de *privacy*
- Il développe et gère la politique en matière de sécurité de l'information et *privacy*[45]

Ce service s'apparente à un organe de contrôle interne compétent pour contrôler tout projet devant mettre en place un traitement de données à caractère personnel dans le cadre des activités du SPF Finances.

Avant d'aller plus loin, il convient de relever que le paradigme du contrôle a changé avec l'apparition du DPO. En effet, les anciens comités sectoriels avaient une position externe par rapport aux demandes d'autorisation qui lui étaient faites en matière d'échanges de données. Depuis l'adoption du RGPD, le contrôle portant sur les protocoles d'encadrement de transfert de données à caractère personnel intervient, en premier lieu, par les soins du DPO assisté par le Service Privacy. Certains pourraient critiquer ce système en considérant que le DPO et le Service Privacy font parties intégrantes du SPF Finances, de sorte qu'ils ne sont ni l'un, ni l'autre, indépendants et impartiaux. Ils pourraient donc être vus comme juges et parties dans le cadre des traitements des données à caractère personnel[46]. Néanmoins, cette organisation du contrôle suit l'objectif de responsabilisation des acteurs en charge de traitement des données à caractère personnel, comme nous le verrons *infra*.

Pour répondre à la position controversée du Service Privacy, on pourrait arguer que l'article 5 §2 de la loi du 3 août 2012 prévoie que toute intégration de données provenant de tiers dans le datawarehouse du SPF Finances doivent faire l'objet d'une délibération de la chambre compétente du Comité de Sécurité de l'information (ci-après CSI). Cette faculté de

---

[45] https://finances.belgium.be/fr/sur_le_spf/structure_et_services/services_du_president/privacy, consulté le 13 mai 2021 à 14h14.

[46] Dans un arrêt 51/2014 du 27 mars 2014, la Cour Constitutionnelle aurait pu traiter des questions relatives à l'indépendance, l'impartialité et l'efficacité de ce Service mais elle a déclaré irrecevable le moyen tiré de l'article 8 de la loi du 3 août 2012. Pour plus de détails, voy. E. DEGRAVE et. A. LACHAPELLE, « Le droit d'accès du contribuable à ses données à caractère personnel et la lutte contre la fraude fiscale », *R.G.C.F.*, 2014/5, p.329.

contrôle pourrait éventuellement atténuer le questionnement sur l'indépendance et l'impartialité relative au Service Privacy.

d. Le Comité de Sécurité de l'information et les protocoles

Concernant spécifiquement la mise en place du Comité de sécurité de l'information, on peut s'apercevoir que le législateur a opéré un rétropédalage. A cet effet, le Conseil d'Etat avait déjà dénoncé cette incohérence dans son avis du 26 avril 2018[47]. En effet, le RGPD a consacré le principe *d'accountability,* qui a pour but de responsabiliser les responsables de traitement. C'est dans cet ordre d'idées que le législateur belge a mis fin au système des formalités préalables aux traitements de données, en abrogeant les mécanismes d'autorisation des Comités sectoriels. Cependant, lorsqu'on analyse la loi du 5 septembre 2018, le législateur semble être revenu en arrière, dans la mesure où il a fait « renaître » les Comités sectoriels pour la sécurité sociale, ainsi que celui pour l'autorité fédérale, compétent pour le SPF Finances. Le législateur a fait renaître ces comités par le biais des chambres compétentes du Comité de Sécurité pour l'information. Ainsi, soumettre à un examen de légalité préalable une communication de données à caractère personnel à la chambre de l'autorité fédérale du CSI contreviendrait d'une part, au principe d'*accountability* consacré par le RGPD et d'autre part, au système des protocoles d'échanges prévus par la LTD[48].

e. Les problèmes liés aux sanctions

L'article 20 14° de la LPD prévoit une certaine latitude dans le chef des responsables de traitement au regard des mesures visant à sanctionner la violation d'un protocole mais ce, sans préjudice du titre 6 de la LTD concernant les sanctions administratives et pénales.

Néanmoins, ce système a fait l'objet d'une critique puisque la Cour constitutionnelle a été saisie d'un recours en annulation de l'article 221 §2 de la LPD adopté en application de l'article 83 du RGPD prévoyant l'imposition d'amendes administratives[49]. L'article 221 §2 exonère de sanctions administratives les autorités publiques n'exerçant pas une

---

[47] Avis n° 63.202/2, donné le 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 ».

[48] L. GERARD, *op. cit.,* p. 61.

[49] C. Const., n°3/2021 du 14 janvier 2021.

activité d'offre de biens et services sur un marché. Le Conseil d'Etat n'avait pas manqué d'interpeller le législateur quant à cette exonération lors de l'avis précédent l'adoption de la loi[50].

En l'espèce, les requérants demandaient l'annulation de l'article 221 paragraphe 2 de la loi du 30 juillet 2018 au motif que celui-ci était contraire aux articles 10 et 11 de la Constitution lus en combinaison avec les articles 7, 8, 20, 21 paragraphe 1, et 52 paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne, avec l'article 16 § 1 du TFUE, avec le principe général d'égalité et non-discrimination en droit de l'Union européenne, avec l'article 8 de la Convention européenne des droits de l'Homme et avec les articles 83 et 84 du RGPD, en ce qu'il exonère les autorités publiques du régime des sanctions administratives prévues par le RGPD en cas de violation de celui-ci sauf si ces autorités publiques agissent sur un marché en offrant des biens et des services.

Les requérants estiment ici qu'il existe une différence de traitement injustifiée en raison du fait que les entreprises privées et les autorités publiques sont soumises de la même manière à des obligations en matière de protection des données, alors qu'elles ne sont pas soumises au même traitement en cas de non-respect des obligations. En l'occurrence, la disposition attaquée paralyse l'action de l'Autorité de protection des données, puisque cette dernière se retrouve dans l'impossibilité d'imposer des sanctions administratives.

La Cour a rejeté le moyen au terme d'un raisonnement en plusieurs étapes : initialement, la Cour a rappelé le principe général selon lequel une différence de traitement n'est possible que si elle est objectivement justifiée, c'est-à-dire qu'elle repose sur des critères objectifs et qu'elle doit respecter le principe de proportionnalité (B.25. alinéa 1). En l'occurrence, la Cour admet la similarité des activités entre secteur public et secteur privé au niveau des traitements de données à caractère personnel, notamment en rappelant la notion *erga omnes* de responsable de traitement, applicable tant au secteur privé qu'au secteur public (B.24.2). La Cour estime que l'exception vise certaines autorités publiques, catégorisées sur la base de deux critères objectifs, à savoir la qualité de la personne morale de droit public et l'activité, c'est-à-dire l'offre de biens et services sur un marché (B.26.1). A cet égard, elle estime également qu'en ce qui concerne la qualité, il faut vérifier si la personne morale et ses

[50] M. KNOCKAERT, *op.cit.*, p. 22 voy. Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, M.B., 5 septembre 2018, p. 68616, p. 21.

mandataires n'effectuent que des missions de service public, en ce qu'elles servent l'intérêt général. C'est en cela qu'elle se distingue de la personne morale de droit privé. Quant au critère de l'activité, les travaux préparatoires de la loi définissent par offre de biens et services, la possibilité pour des personnes morales d'entrer en concurrence avec des acteurs privés soumis aux obligations du RGPD (B.27.1 et B.27.2). Les travaux préparatoires de la loi témoignent du fait que l'exception a été prévue au motif de ne pas mettre en péril la continuité du service public en raison du poids financier qu'il pourrait engendrer.

En outre, au regard de l'architecture des mesures correctrices adoptées par le RGPD, la Cour a souligné que l'imposition d'amendes administratives ne constituent pas le seul moyen de sanctionner une violation des obligations en matière de protection des données à caractère personnel. A cet effet, la Cour a rappelé que le système des sanctions administratives ne constitue qu'un moyen indirect de correction puisque le RGPD prévoit des remèdes directement bénéficiables aux individus concernés par le biais d'un mécanisme d'indemnisation de dommages et intérêts, contenu dans l'article 82 du RGPD, applicable indistinctement aux entreprises privées qu'aux autorités publiques[51].

f. Les autres mesures techniques et organisationnelles du SPF Finances

i. L'IAM (Identification Access Management)

L'IAM *(Identification Access Management)*, est consacré à l'article 10 de la loi du 3 août 2012. Conformément à cet article, le DPO, assisté par les agents de son service, contrôle le fonctionnement de ce réseau IAM. De cette manière, le DPO et le Service Privacy contrôlent, d'une part, les accès physiques aux différents bâtiments de travail du SPF Finances par le biais de badges électroniques et, d'autre part, les accès aux différentes bases de données dont l'administration est responsable du traitement, du fonctionnement et de la protection. Grâce à ce réseau IAM, il est possible pour les agents du Service Privacy d'établir une traçabilité des activités de chaque agent du SPF Finances par le biais de ce qu'on dénomme des journaux d'accès.

ii. Le PIA (Privacy impact assessment)

Lors d'un projet d'échange de données nécessitant un traitement de données à caractère personnel, l'article 35 du RGPD prévoit une obligation de PIA (*Privacy impact*

[51] C.Const. op. cit. cons. B.28. à B.30.

assessment) ou AIPD (Analyse d'impact sur la protection des données). Cette obligation consiste à opérer, dans le chef du responsable de traitement, une analyse quant aux impacts d'un traitement de données à caractère personnel sur les droits et les libertés des personnes concernées. Toutefois, le RGPD prévoit une modulation pour le secteur public consacrée à l'article 35.10 du RGPD. Conformément à cet article, le responsable de traitement est exonéré de l'obligation de d'analyse d'impact si celle-ci a été réalisée en amont dans la discussion et l'adoption de la base juridique autorisant le traitement, à moins que les Etats membres n'estiment nécessaire de maintenir cette analyse d'impact. Le législateur belge a utilisé la possibilité de l'article 35.10 du RGPD en l'article 23 de la LPD, puisqu'il enjoint les autorités publiques à opérer une analyse d'impact spécifique sur l'activité de traitement concernée[52]. Ces exigences de PIA semblent également s'appliquer au sein du SPF Finances à tout le moins au niveau des activités de profilage[53]. A cet effet, l'Autorité de Protection des données rappelle les trois principaux cas dans lesquels un PIA est exigé conformément à l'article 35.3 du RGPD, à savoir : une évaluation d'aspects personnels telle que le profilage, suivie d'une décision sur une personne physique, un traitement à grande échelle de données particulières prévues aux articles 9 et 10 et, une surveillance systématique à grande échelle d'une zone accessible au public[54].

g. Brève conclusion

Comme nous l'avons analysé, la matière des échanges de données entre administrations est une matière complexe et en perpétuel mouvement. En effet, le développement des règles en cette matière suit le développement technologique et l'évolution numérique. A cet égard, le droit à la vie privée des contribuables doit être protégé de manière dynamique, en tenant compte des missions légales des autorités fiscales mais aussi en respectant les exigences tenant à la légalité des ingérences dans la vie privée. De nos jours, les idéaux de droit à la vie privée et de lutte contre la fraude peuvent se heurter, en particulier dans le contexte actuel du coronavirus.

---

[52] M. KNOCKAERT, *op. cit., p23.*
[53] S. DE RAEDT, *op. cit.*, p. 132.
[54] https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/analyse-d-impact-relative-a-la-protection-des-donnees, consulté le 5 mai 2021 à 15h57.

IV. PARTIE 3: LES NOTIONS DE DATAWAREHOUSE, DATAMINING, DATAMATCHING ET PROFILAGE

La problématique des échanges de données à caractère personnel et, plus largement, la circulation des données à caractère personnel est un enjeu majeur dans le contexte de crise sanitaire que nous connaissons à cause du coronavirus. En effet, les différentes entraves aux libertés individuelles prises par le gouvernement ont été palpables. A cet égard, la crise sanitaire a eu l'effet de remettre sur le devant de la scène la question de la protection des données à caractère personnel et de la compatibilité des traitements opérés par les administrations avec le droit à la vie privée des citoyens. Plus précisément, nous allons analyser les procédés informatiques de datamatching, datamining et de profilage utilisés par certaines autorités publiques (principalement, le SPF Sécurité Sociale et le SPF Finances) et ce, dans un datawarehouse, afin de les confronter aux normes protectrices de la vie privée et des données à caractère personnel.

1) La notion de datawarehouse

a. Définition

Dans son sens commun, un datawarehouse renvoie à l'expression française d'« entrepôt de données ». La notion est définie à l'article 5 §1er 1° de la loi du 3 août 2012[55]. En termes techniques, Un *datawarehouse « est une plateforme utilisée pour collecter et analyser des données en provenance de multiples sources hétérogènes »*[56]. En d'autres termes, un datawarehouse consiste donc en une masse de données sur lesquelles on peut procéder à des analyses. Le datawarehouse du SPF Finances n'est pas le seul à être mis en place au sein des administrations belges. En effet, l'ONSS au sein du SPF Sécurité Sociale dispose d'un outil similaire que l'on appelle OASIS[57]. Le datawarehouse OASIS, outil très efficace contre la fraude sociale, fait néanmoins l'objet de critiques quant à sa compatibilité avec plusieurs droits

[55] Article 5 §1er 1° libellé comme suit : « "datawarehouse": un système de données contenant une grande quantité de données numériques pouvant faire l'objet d'une analyse; »
[56] https://datascientest.com/data-warehouse, consulté le 12 mai 2021, à 9h34.
[57] Acronyme désignant « Organisation Antifraude des Services d'Inspection sociale » voy. not. sub. pag. E. DEGRAVE, « « Les citoyens contrôlés via leurs données Covid ? Le datamatching et le datamining utilisé par l'Etat », J.T. 2021/7, n°6845.

fondamentaux, notamment le droit à la vie privée et le droit à la transparence de l'administration[58].

b. La controverse autour du datawarehouse

Concernant la création d'un *datawarehouse* au sein du SPF Finances, une critique avait déjà été mise en 2014 concernant la mise en place d'un datawarehouse. En effet, la loi manquait déjà de précisions quant à la provenance des données des contribuables et à la possibilité pour les contribuables de corriger les données se trouvant sur ce *datawarehouse*[59]. En 2018 également, lors de la mise en œuvre des principes du RGPD, la section Législation du Conseil d'Etat s'était montrée critique vis-à-vis de cette masse systémique de données[60]. En effet, la section Législation estime qu'il appartient au législateur de fixer avec précision les catégories de données mises à disposition du SPF Finances au sein de ce *datawarehouse* ainsi que les finalités pour lesquelles les données pourraient être traitées. En outre, il appartient également au législateur de prévoir avec précision les modalités de collecte et *« les éléments permettant de vérifier la pertinence et la nécessité de l'intégration de ces données à caractère personnel, ainsi que la durée de conservation de celles-ci, le responsable du traitement, les personnes autorisées à consulter la base de données et les conditions de réutilisations de données traitées. On ignore également si la réutilisation de données qui est ainsi envisagée sera faite à des fins distinctes de celles pour lesquelles elles ont été collectées »*[61]. A en croire l'avis de la section législation du Conseil d'Etat, la situation ne semble pas avoir changé depuis l'adoption de la loi du 3 août 2012 puisque des critiques demeurent autour des règles qui encadrent le fonctionnement du *datawarehouse* et les traitements de données à caractère personnel qui y sont opérés.

2) Le *datamatching*, le *datamining* et le profilage

Le *datamatching*, en français « couplage de données » consiste à regrouper des données figurant sur un datawarehouse et à les comparer entre elles. La notion est définie à l'article 5 §1er 3° de la loi du 3 août 2012 comme *« la comparaison entre plusieurs sets de données rassemblées »*. Le *datamining*, en français « extraction de données », consiste en

[58] voy. E. DEGRAVE, « The use of secret algorithms to combat social fraud in Belgium », *European Review of Digtital Administration & Law*, 2020, pp. 167-177
[59] E. DEGRAVE et. A. LACHAPELLE, « Le droit d'accès du contribuable à ses données à caractère personnel et la lutte contre la fraude fiscale », *R.G.C.F.*, 2014/5, p.332.
[60] Avis n° 63.202/2, rendu le 28 avril 2018.
[61] L. RENDERS et al., « Le Conseil d'Etat, chronique de légisprudence 2018 », *R.B.D.C*, 2020/2, p.186, n°21.

l'opération postérieure, à savoir l'opération sur base de laquelle on va appliquer des algorithmes qui vont permettre de faire ressortir des données nouvelles. Le *datamining* est défini à l'article 5 §1er 4° de la loi du 3 août 2012 comme *«la recherche de manière avancée d'informations dans de gros fichiers de données »*. C'est grâce à ce processus qu'il est possible d'effectuer des activités de profilage. Le profilage consiste à prendre une décision sur base d'un traitement automatisé de données[62]. A cet égard, l'article 5 §1er al 1er de la loi du 3 août 2012 renvoie simplement à la définition contenue à l'article 4.4 du RGPD. Afin d'illustrer notre propos, E. DEGRAVE propose cet exemple théorique : *« En guise d'exemple simple, prenons le cas de John, dont les données fiscales montrent qu'il gagne 2.000 EUR par mois. Or, ses données à la DIV montrent qu'il détient 7 Ferrari neuves. Le Registre national indique qu'il est propriétaire de deux châteaux. Les algorithmes « anti-fraude » vont cibler John. Il sera rattaché à la catégorie des présumés fraudeurs fiscaux et sociaux et un contrôle fiscal et/ou social sera encouragé. »*[63]

En ce qui concerne le profilage et la prise de décision sur base d'un traitement automatisé, la loi du 3 août 2012 semble indécise. En effet, bien que le SPF Finances utilise le traitement automatisé de données dans le cadre de ses investigations, on ne peut admettre pareille affirmation pour ce qui est d'un véritable processus décisionnel automatisé. Pour que le profilage soit considéré comme un processus de décision automatisé, il faut, d'une part, que la décision prise soit le fruit exclusif d'un procédé automatisé sans intervention humaine et, d'autre part, qu'elle produise des effets juridiques dans le chef de la personne concernée. Appliquée aux investigations fiscales, il est clair que la décision produit des effets juridiques puisque le contribuable devra se conformer à un contrôle, par exemple. Néanmoins, il demeure incertain que le processus menant à la décision soit le fruit exclusif du profilage ou s'il y a eu une intervention humaine[64].

Or, l'article 22.1 du RGPD prévoit que la personne concernée, ici le contribuable, a le droit de ne pas être l'objet d'une décision basée exclusivement sur un traitement automatisé y compris le profilage. Néanmoins, L'article 22.2.b du RGPD prévoit

---

[62]Le profilage est défini à l'article 4.4 du RGPD comme : *« toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique; »*

[63] E. DEGRAVE, « Les citoyens contrôlés via leurs données Covid ? Le datamatching et le datamining utilisé par l'Etat », J.T. 2021/7, n°6845.

[64] S. DE RAEDT, *op. cit.*, p.137. voy. également S. DE RAEDT, *De draagwijdte van het recht op privéleven bij de informatie-inzameling door de fiscale administratie*, Gent, Larcier, 2017, p.169-198.

tout de même la possibilité d'adopter une décision si « *elle est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée* ».

Concernant le droit belge à cet égard, l'article 5 §1er de la loi du 3 août 2012 prévoit bien la possibilité du profilage, la réalisation de contrôle ciblés sur base d'indicateurs de risque et l'analyse de données relationnelles provenant d'autres administrations ou du SPF Finances même. Bien que la loi belge prévoie la possibilité du profilage, on ignore toutefois si ce profilage débouche effectivement sur une décision basée purement automatique conformément à l'article 22.2.b. du RGPD en ce qui concerne la prise de décision sur base d'un traitement automatisé en tant que tel[65].

Les différents procédés ont été modernisés et avalisés dans la loi CSI en son article 71. Comme le souligne E. DEGRAVE, la loi CSI du 5 septembre 2018 est une loi qui pose potentiellement question. En effet, la loi ne prévoit pas quelles données sont centralisées et les finalités pour lesquelles elles vont être utilisées. Elle ne prévoit pas non plus un encadrement suffisant pour les opérations de profilage. En matière de sécurité sociale, l'article 61 la loi CSI va même jusqu'à exclure certains droits prévus par le RGPD[66].

Ainsi que nous l'avons mentionné supra, la loi du 5 septembre 2018 a également créé un nouvel organe de contrôle, le CSI. En ce qui concerne le SPF Finances et la problématique des échanges de données, le CSI pourrait, par exemple, sur base de l'article 13 de la loi CSI, utiliser les données récoltées dans le cadre de la campagne de vaccination contre le coronavirus au sein du SPF Sécurité Sociale et les réutiliser en opérant un croisement avec des données fiscales, en faisant des opérations de *datamining*. En outre, le CSI pourrait décider par lui-même, d'injecter des autres données dans le datawarehouse du SPF Finances, dans la mesure où l'article 71 de la loi CSI traduit dans l'article 5 §2 alinéa 1er de la loi du 3 août 2012 lui permet d'adopter une délibération allant dans ce sens. De cette manière, et suite au profilage, un profil type de personne suspectée de fraude sociale et/ou fiscale pourrait être dégagé simplement sur base d'opérations algorithmiques.

---

[65] S. DE RAEDT, *op. cit.*, p. 136.
[66] E. DEGRAVE, *op. cit.*

A titre illustratif, en appliquant ce raisonnement dans le contexte de la collecte des données en raison du coronavirus et des mesures sanitaires, il se pourrait, par exemple, qu'une personne bénéficiant d'allocations de chômage en raison du COVID-19 soit testée positive et qu'on identifie sa contamination sur un chantier de construction. Les données recueillies pourraient potentiellement servir à automatiquement considérer la personne comme suspectée de fraude sociale en raison d'un éventuel emploi au noir. En outre, ce type d'informations et de processus ne seraient pas sans intérêts pour l'administration fiscale ces informations pourraient servir à effectuer une taxation sur base des revenus réels de la personne et non sur base du montant perçu par le biais de l'octroi des allocations de chômage. En effet, les revenus d'un travail au noir entrent dans la catégorie des revenus illicites qui entrent en ligne de compte dans la détermination du revenu net nécessaire à l'établissement de l'impôt.

A la lecture de l'état actuel du droit et dans le contexte sanitaire que nous connaissons, la compatibilité du système prévu par la loi CSI avec l'article 22 de la Constitution et les normes supranationales protectrices de la vie privée et des données à caractère personnel semble poser question.

V. CONCLUSION

Comme nous avons pu l'analyser, le développement technologique et l'avènement du numérique ont modifié les méthodes de travail des administrations. L'échange de données entre administration et la circulation des données à caractère personnel entre les autorités publiques est devenu la norme après une longue période de cloisonnement. Cependant, la numérisation et la multiplication croissante de ces échanges n'est pas à prendre à la légère. Dans certains cas, il peut y avoir des violations du droit à la vie privée, qui peuvent passer inaperçues en raison de l'inflation législative latente. Après avoir esquissé une architecture globale de la protection des données en Belgique, nous avons tenté de démontrer que ces dispositions sont capitales pour régir la relation entre l'administration et les citoyens. Certes, nous savons que le droit fondamental à la vie privée des contribuables, et des citoyens en général, n'est pas un droit absolu, encore moins dans le contexte de crise sanitaire que nous connaissons. Il n'en demeure pas moins que l'administration ne peut pas tout faire, bien qu'elle puisse parfois poursuivre des objectifs louables comme la lutte contre le coronavirus ou bien la lutte contre la fraude.

A cet égard, nous avons mis en exergue les problèmes et les dangers en termes d'entraves à la vie privée lorsque nous avons vu les incohérences du système des protocoles, le rôle et l'encadrement du CSI, ainsi que des procédés de *datamatching*, *datamining* et profilage. Ces éléments témoignent d'une certaine atteinte du droit à la vie privée des citoyens au sens large.

Les diverses analyses témoignent donc de la nécessité de la mise en place de garde-fous et de la vigilance qui doit animer tout contribuable et tout citoyen au sens large. Cela témoigne également du rôle crucial que vont jouer l'Autorité de protection des données et les juridictions dans la relation entre les autorités publiques et les administrés. Les différentes juridictions du pays vont être confrontées (ou le sont déjà) à ce mariage entre le droit à la vie privée du contribuable et les pouvoirs de l'administration fiscale, dans un contexte numérique et de crise sanitaire, afin de parvenir à un fragile, mais juste équilibre.

BIBLIOGRAPHIE

Doctrine

T. AFSCHRIFT, « GDPR: Un système à la mesure du fisc ! », *Sem. Fisc.* 2018/37, n°351, p.1. disponible sur https://www.idefisc.be/view-article.php?idefisc_numero_id=201809

A. BEELEN, « Fiche de guidance n°1 : le champ d'application matériel du RGPD », *Guide pratique du RPGD*, Bruylant, 2018.

S. DE RAEDT, *De draagwijdte van het recht op privéleven bij de informatie-inzameling door de fiscale administratie*, Gent, Larcier, 2017.

S. DE RAEDT, "The impact of the GDPR on Belgian Tax Authorities", *R.D.T.I.*, 2017/1-2.

E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, coll. Crids, Bruxelles, Larcier, 2014, n°492 et s.

E. DEGRAVE, « Section 1 – L'exigence de finalité », in *l'e-gouvernement et la protection de la vie privée*, Bruxelles, Editions Larcier, 2014, pp.178-208.

E. DEGRAVE, « Protection des données et Comités sectoriels : avant et après le RGPD », *R.D.T.I*, 2018/4, n°73, pp. 91-97.

E. DEGRAVE, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.*, 2009, pp. 365-371.

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

E. DEGRAVE, « Les citoyens contrôlés via leurs données Covid ? Le datamatching et le datamining utilisé par l'Etat », *J.T.* 2021/7, n°6845.

E. DEGRAVE, « The use of secret algorithms to combat social fraud in Belgium », *European Review of Digtital Administration & Law*, 2020, pp. 167-177

E. DEGRAVE et. A. LACHAPELLE, « Le droit d'accès du contribuable à ses données à caractère personnel et la lutte contre la fraude fiscale », *R.G.C.F.*, 2014/5, pp. 322-335.

E. DEGRAVE et Y. POULLET, « Entre chasse à la fraude et respect de la vie privée », *Le Soir*, 4 mai 2012.

E. DEGRAVE et Y. POULLET, « Le droit au respect de la vie privée face aux nouvelles technologies », in N. BONBLED et M. VERDUSSEN (dir.), *Les droits constitutionnels en Belgique : les enseignements jurisprudentiels de la Cour constitutionnelle, du Conseil d'État et de la Cour de cassation*, Bruxelles, Bruylant, 2011, p. 1017.

C. DE TERWANGNE, E. DEGRAVE, A. DELFORGE et L. GERARD, *La protection des données à caractère personnel en Belgique : manuel de base*, 2019, Bruxelles, Politeia.

I. DE POORTER, "De GDPR of Algemene Verordening Gegevensbescherming – een algemene inleiding", in *Financiële regulering: een dwarsdoosnede*, Intersentia, 2019.

L. GÉRARD, « Le comité de sécurité de l'information : illustration d'une incohérence législative», *R.D.T.I.*, 2018/4, n° 73, pp.55-72.

L. GÉRARD, « Les sanctions en cas de non-respect du RGPD: vers une plus grande effectivité de la protection des données à caractère personnel ? », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de TERWANGNE et K. ROSIER (coord.), Bruxelles, Larcier, 2018, pp. 641-654

K. JANSSENS et M. NUYTTEN, "De Algemene Verordening Persoonsgegevens: van theorie naar praktijk", R.D.C-T.D.H, 2018/5, pp.401-435.

A. LACHAPELLE, « Chapitre 1 – la lutte contre la fraude et l'évasion fiscale à l'ère de la transparence », in *La dénonciation à l'ère des lanceurs d'alerte fiscale*, Larcier, Collection du Crids, 2021

A. LACHAPELLE, « Chapitre 2 – La reconfiguration des limites de la dénonciation au regard des droits fondamentaux », in *La dénonciation à l'ère des lanceurs d'alerte fiscale*, Bruxelles, Larcier, 2021, p.986-1179.

M. KNOCKAERT, « La loi du 30 juillet 2018 : l'échange de données à caractère personnel dans le secteur public », *R.D.T.I,* 2019/1, n°74, pp. 5-24.

F. LEDAIN, « La protection des PC à l'occasion d'un contrôle fiscal », *Sem. Fisc.*, 2018/18.

T. LEONARD et Y. POULLET, « Titre 3 – L'intérêt général comme arbitre du débat vie privée v. liberté d'expression dans le RGPD », in *Vie privée, liberté d'expression et démocratie dans la société numérique,* Bruxelles, Editions Larcier, 2020, pp. 73-122.

F-S. MEEÛS et E. TRAVERSA, « III.5 – Droit à la vie privée et à liberté d'expression », in *Les grands arrêts de la jurisprudence fiscale*, 2020, pp.248-295.

N. MICHAIL, « Le domaine d'application du GDPR : de sa portée hors de l'Union et de sa mise en œuvre dans l'Union », *R.D.C.-T.B.H.*, 2019/1, p.52-79.

P. RACINE, « Un essai de vue d'ensemble de la protection des données personnelles en matière fiscale », *R.E.I.D.F.*, 2018/2, pp. 279-288.

L. RENDERS et al., « Le Conseil d'Etat. chronique de légisprudence 2018 », *R.B.D.C*, 2020/2, pp. 169-301.

B. SALOVIC, O. GERGUINOV et T. LÉONARD, « Sous couvert de sécurité, la loi belge viole-t-elle le RGPD ? », 12 septembre 2018, accessible sur https://www.lexology.com/library/detail.aspx?g=ffb23fd6-1277-4ce6-9df8-acbdaedeb397

C. SEILLÈS, « L'échange automatique de renseignements en matière fiscale », *D.B.F/B.F.R.*, 2016/16.

V. SÉPULCHRE, « Les droits de l'homme et les droits fondamentaux dans le droit fiscal belge : évolutions des dernières années », *R.G.C.F.*, 2009/6, p.525-p.584.

J. SOETAERT, « L'échange de données financières coulée dans une loi belge », *Sem. Fisc.*, 2016/8, n°227, pp. 4-5.

L. TASSONNE, « La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme », in *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Editions Larcier, 2015.

O. TAMBOU, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020.

V. VERBRUGGEN, « Titre 1: RGPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne », in *Le Règlement général sur la protection des données (RGPD/GDPR)*, p.27.

S.D. WARREN et L. BRANDEIS, *The Right to Privacy*, Harvard Law Review, vol. 4, n° 5, 15 décembre 1890, pp. 193-220.

V. WÖHRER, *Data Protection and Taxpayers Rights : Challenges Created by Automatic Exchange of Information*, Amsterdam, IBFD, 2018.

Jurisprudence

1) Cour constitutionnelle

C. Const, arrêt n° 51/2014 du 27 mars 2014.

C. Const, arrêt n° 108/2016 du 14 juillet 2016.

C. Const., arrêt n° 29/2018 du 15 mars 2018.

C. Const., arrêt n°153/2018, 8 novembre 2018.

C. Const., arrêt n° 2/2021 du 14 janvier 2021.

C. Const., arrêt n°3/2021 du 14 janvier 2021.

2) Conseil d'Etat

- Avis n° 63.192/2, donné le 19 avril 2018, ur un avant-projet devenu la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
- Avis n°63.202/2, donné le 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 ».

3) Commission pour la Protection de la Vie Privée (C.P.V.P)/ Autorité de protection des données (A.P.D.)

Comité sectoriel pour l'Autorité fédérale, Délibération AF n°39/2017 du 14 décembre 2017, pp.5-8.

C.P.V.P, Recommandation n°2/2012 du 8 février 2012 relative aux principes de bases à respecter lors de traitements de données à caractère personnel impliquant le SPF Finances

C.P.V.P, avis n°11/2012 du 11 avril 2012 relatif à l'avant-projet de loi relatif aux traitements de données à caractère personnel réalisés par le Service Public Fédéral Finances dans le cadre de ses missions, p.9, n°29.

4) C.E.D.H

C.E.D.H, *Rotaru c. Roumanie,* 4 mai 2000, req. n° 28341/85.

C.E.D.H, 26 mars 1987, *Leander c. Suède*, req. n° 9248/81.

C.E.D.H, Gr. ch, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, req. n° 30562/04 et 30566/04.

C.E.D.H., 17 décembre 2009, *B.B. c. France*, req. n° 5335/06.

C.E.D.H, 10 février 2011, *Dimitrov-Kazakov c. Bulgarie*, req. n° 11379/03.

C.E.D.H.,18 octobre 2011, *Khelili c. Suisse*, req. n° 16188/07.

C.E.D.H., 9 octobre 2012, *Alkaya c. Turquie*, req. n° 42811/06.

C.E.D.H., 18 avril 2013, *M.K. c. France*, req. n° 19522/09.

C.E.D.H., 18 septembre 2014, *Brunet c. France*, req. n°12662/06.

5) C.J.U.E

C.J.U.E. (3e ch.), 1er octobre 2015, *Smaranda Bara*, C-201/14.

Législation belge

Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p.5801.

Loi du 3 août 2012 portant des dispositions relatives aux traitements de données à caractère personnel réalisés par le Service Public fédéral Finances dans le cadre de ses missions, *M.B.* 24 août 2012, p. 50670.

Loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, *M.B.* 29 août 2012 p.53170.

Loi du 14 juin 2017 modifiant l'article 36bis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.* 28 juillet 2017, p. 75932.

Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.* 10 janvier 2018, p. 989.

Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.* 5 septembre 2018, p. 68616.

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*, M.B.* 10 septembre 2018, p. 69589.

Législation européenne

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOUE, L.281, 23 novembre 1995, pp.31-50.

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 (règlement général sur la protection des données