L'INTÉGRATEUR DE SERVICES FÉDÉRAL AU CŒUR DE LA SIMPLIFICATION ADMINISTRATIVE

par

Elise DEGRAVE*
Chargée de cours à la Faculté de droit de l'Université de Namur
Post-doctorante à la Chaire E-gouvernement
et au Centre de recherches Information Droit et Société (CRIDS)

SOMMAIRE

INTRODUCTION

Une loi du 15 août 2012 crée et organise un « intégrateur de services fédéral ».

Face à pareille créature institutionnelle, les publicistes oscillent généralement entre curiosité et crainte. Quant aux spécialistes du droit des technologies, s'ils se réjouissent souvent de constater l'étendue progressive d'outils informatiques qui leur sont familiers, leur enthousiasme peut se heurter à des problématiques de droit public qui les rendent plus mal à l'aise.

Un constat naît alors : l'e-gouvernement, qui désigne l'usage des technologies dans l'administration et que l'on appelle également « administration électronique », est largement délaissé par la doctrine en droit public et en droit des technologies. En outre, les règles qui encadrent ce phénomène récent sont peu connues des avocats et des magistrats et sont donc trop peu exploitées. Enfin, les citoyens tout à la fois se réjouissent de constater un allègement de leurs démarches administratives mais craignent l'usage qui sera fait de leurs données personnelles.

C'est pourquoi, la présente étude entend faire la lumière sur des aspects cardinaux de l'e-gouvernement au départ d'une analyse d'un outil emblématique de l'administration contemporaine qu'est l'intégrateur de services fédéral.

I. L'ADMINISTRATION BOULEVERSÉE PAR LES TECHNOLOGIES

1. DE L'ADMINISTRATION EN SILOS À L'ADMINISTRATION EN RÉSEAUX

L'informatisation de l'administration n'est pas une simple modernisation de celle-ci. Le déploiement des technologies dans le secteur public n'aboutit pas seulement à remplacer les fichiers de papiers par des bases de données électroniques et à permettre l'envoi de courriels plutôt que de courriers postaux. L'administration est aujourd'hui profondément bouleversée par les technologies, dans son fonctionnement, mais également dans sa structure.

En effet, longtemps, l'administration était structurée en silos. Les institutions publiques œuvraient de manière cloisonnée, collectaient auprès des citoyens les informations dont elles avaient besoin pour l'exécution de leurs propres missions et ne les partageaient pas ensuite. Il en résultait une perte de temps et d'argent pour l'administration, qui devait contacter chaque personne pour chaque information nécessaire, attendre sa réponse, réclamer éventuellement des précisions, 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

* L'auteure remercie Luc Van Tilborgh, Program Manager au SPF Fedict, ainsi que Benoît Wanzoul, Directeur de la Banque-carrefour d'échanges de données, pour leur aide précieuse. Néanmoins, les opinions défendues dans cet article n'engagent qu'elle-même.

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 l'apparition de l'informatique, on constate que les administrations peuvent désormais collaborer efficacement. La volonté naît alors d'encourager les « synergies entre les divers services et niveaux des pouvoirs publics »[1], dans le but de simplifier les démarches et procédures administratives. L'informatique 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[2].

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

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

Ensuite, différentes administrations se voient attribuer la responsabilité de collecter, enregistrer et mettre à jour certaines données déterminées. Les bases de données contenant ces informations et placées chacune sous la responsabilité d'une administration sont appelées « sources authentiques de données »[3]. L'idée est de faire en sorte que chaque information relative au citoyen ne soit enregistrée qu'une seule fois par une seule administration du réseau, qui est ensuite responsable de la fiabilité de ces données.

Enfin, on place, au cœur de ce réseau d'administrations, un outil d'un type nouveau : l'intégrateur de services, dit aussi « plateforme d'échange d'informations » ou encore « banque-carrefour ». En somme, l'intégrateur de services est une infrastructure technique, placée au cœur d'un réseau d'administrations, et qui est chargée d'assurer, au sein de ce réseau, l'échange électronique d'informations provenant de sources authentiques diverses. Ainsi, lorsqu'une administration a besoin d'une donnée dont elle ne dispose pas, il lui suffit de s'adresser à l'intégrateur de services qui contacte l'administration détentrice de la donnée recherchée et l'achemine ensuite vers l'administration qui la lui a demandée.

Afin de faciliter la compréhension de l'exposé, on peut, d'ores et déjà, schématiser comme suit le modèle d'un réseau d'administrations comprenant un intégrateur de services.

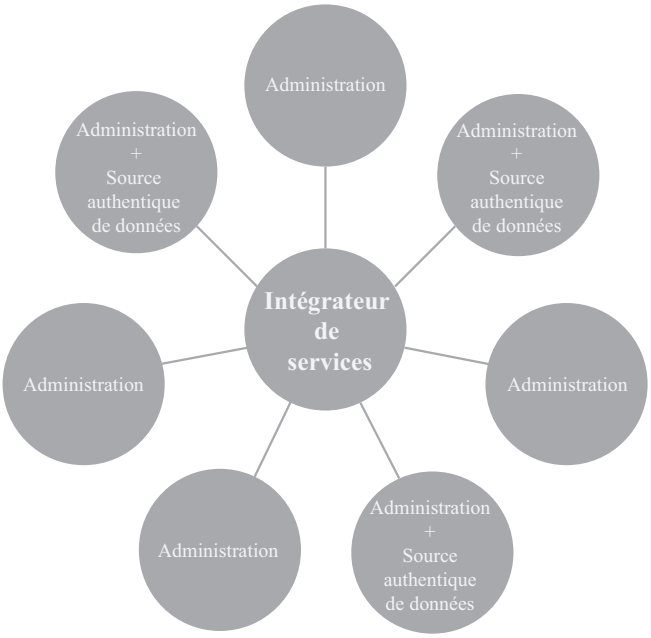


Schéma illustrant un réseau d'administrations composé d'un intégrateur de services auquel sont reliées plusieurs administrations dont certaines détiennent une source authentique de données.

2. PLUSIEURS RÉSEAUX D'ADMINISTRATIONS ET INTÉGRATEURS DE SERVICES

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

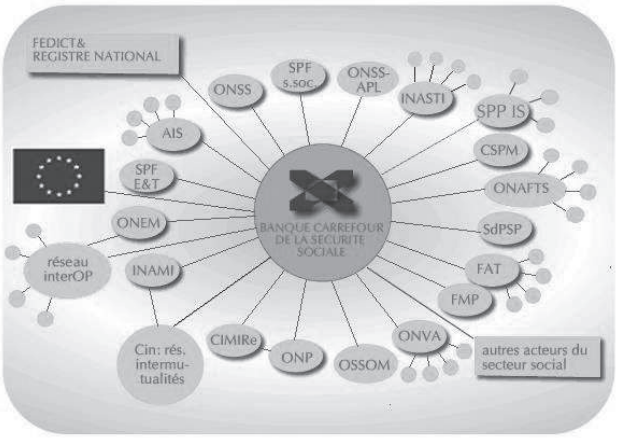
Les premiers réseaux créés sont des réseaux dits « sectoriels », car ils sont liés à un domaine particulier de l'administration. L'intégrateur de services placé au cœur de ces réseaux sectoriels est qualifié d'intégrateur « vertical » par opposition aux intégrateurs de services « horizontaux » décrits ci-après. Le premier réseau du genre est

[1] 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.

[2] 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*, Bruxelles, Larcier, coll. Crids, 2014, en particulier n^{os} 172 et s. Voy. *infra,* n° 3.

[3] Nous revenons ultérieurement plus en détails sur cette notion. Voy. *infra,* II, n° 3.

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 nonante[4]. S'en est suivie la création, en 2008, du réseau sectoriel de la santé, au sein duquel la plate-forme *eHealth* assume le rôle d'intégrateur de services[5].



Exemple d'intégrateur de services vertical : la Banque-carrefour de la sécurité sociale, placée au cœur du réseau de la sécurité sociale

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

Dès lors, dans un deuxième temps et depuis peu, des réseaux et intégrateurs de services dits « horizontaux » ou encore « transversaux » sont mis en place. Ces réseaux regroupent des administrations en fonction de leur appartenance à l'entité fédérale ou à une entité fédérée. Ils comprennent un intégrateur de services chargé d'assurer la circulation des données entre les administrations concernées. Ainsi, en 2012, est créé l'intégrateur de services fédéral, qui sera étudié dans les pages qui suivent. Au niveau des entités fédérées, l'intégrateur de services flamand est créé en 2012 pour assurer l'échange électronique des données au sein du réseau flamand constitué des institutions de la Communauté flamande et de la Région flamande[6]. Il s'agit du « Coördinatiecel Vlaams e-government » (CORVE). Les administrations de la Communauté française et de la Région wallonne sont également regroupées dans un réseau au sein duquel œuvre, depuis 2013[7], un intégrateur de services, dénommé « Banque-carrefour d'échanges de données » (BCED). Grâce à ces intégrateurs horizontaux, les administrations peuvent s'adresser à l'intégrateur de services de l'entité dont elles font partie (État fédéral, Communauté française et Région Wallonne, Communauté flamande et Région flamande), sans devoir s'interroger sur le type de données recherché pour identifier leur interlocuteur. L'intégrateur se charge ensuite d'acheminer l'information recherchée vers l'administration qui l'a demandée, au besoin en contactant lui-même les intégrateurs de services verticaux que sont la Banque-carrefour de la sécurité sociale et la plate-forme *eHealth*.

3. AVANTAGES POUR L'ADMINISTRATION ET POUR LE CITOYEN

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

[4] 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 ».

[5] 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.

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

[7] Décret du 4 juillet 2013 portant assentiment de l'accord de coopération entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.*, 23 juillet 2013.

[8] Pour de plus amples précisions sur la technique du profilage, voy. Recommandation CM/Rec(2010)13 du Comité des Ministres du Conseil de l'Europe aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, disponible sur le site www.coe.int ; M. HILDEBRANDT, « Who is Profiling Who ? Invisible Visibility », in *Reinventing Data Protection ?* (S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE et S. NOUWT (ed.), *Dordrecht*, Springer, 2009, p. 241 ; V. PAPAKONSTANTINOU, « A Data Protection Approach to Data Matching Operations Among Public Bodies », *International Journal of Law and Information Technology,* 2001, vol. 9, n° 1, pp. 62-63 ; J.-M. DINANT,

Le citoyen voit également ses tâches facilitées. Il peut accéder à nombre d'informations en ligne et effectuer des transactions administratives à tout moment depuis son ordinateur. Il est également épargné de certaines démarches administratives grâce à l'automatisation des procédures. À cet égard, par exemple, une application informatique créée par l'intégrateur de services fédéral et dénommée *Ebirth* facilite l'échange des données relatives à la naissance d'un enfant. Ce service part du constat que tant les communes que la Communauté française et le SPF Économie ont besoin d'informations relatives à chaque naissance. Jadis, ces administrations obtenaient ces informations via des formulaires en papier envoyés par les hôpitaux. Aujourd'hui, les hôpitaux se connectent au portail *Ebirth*, encodent les données requises, et celles-ci sont acheminées respectivement vers les communes, la Communauté française et le SPF Économie[9].

II. LE PANORAMA DU RÉSEAU FÉDÉRAL COMPRENANT L'INTÉGRATEUR DE SERVICES FÉDÉRAL

1. LA LOI DU 15 AOÛT 2012 RELATIVE À LA CRÉATION ET À L'ORGANISATION D'UN INTÉGRATEUR DE SERVICES FÉDÉRAL[10]

L'intégrateur de service fédéral est, comme on l'a dit précédemment, un intégrateur de services horizontal, qui assure l'échange des données entre les administrations du réseau fédéral[11].

De facto, le fonctionnement de cet intégrateur de services a commencé vers 2001. À l'époque, aucune loi n'encadrait cet outil informatique. Cette situation était problématique, notamment au regard de la protection de la vie privée des citoyens. En effet, puisque l'intégrateur de services assure l'échange des données à caractère personnel des citoyens entre différentes administrations, il effectue des traitements de données à caractère personnel. Or, chaque traitement de données à caractère personnel est une ingérence dans la vie privée des personnes concernées[12]. En vertu de l'article 22 de la Constitution, ces ingérences doivent être encadrées par une loi précise et prévisible, qui détermine les éléments essentiels des traitements de données. C'est pourquoi, une loi encadrant l'intégrateur de services fédéral a été adoptée le 15 août 2012, mettant fin à cette lacune législative qui persistait depuis plusieurs années. Elle a été rédigée en tenant compte des avis de la Commission de la protection de la vie privée et de la section de législation du Conseil d'État et s'avère globalement satisfaisante. A l'heure actuelle, des arrêtés royaux d'exécution sont encore en cours de rédaction pour préciser certaines notions de la loi.

La présente contribution se concentre à présent sur certains changements que connaît l'administration fédérale à l'heure des technologies, en analysant les traits saillants de l'intégrateur de services fédéral. En particulier, on aborde les questions de savoir quelles administrations sont concernées par cet outil, quelles sont les obligations nouvelles qui leur sont imposées, et quelles sont les sanctions applicables en cas de non-respect de ces règles nouvelles.

2. LE SERVICE PUBLIC FÉDÉRAL FEDICT ET LES SERVICES PUBLICS PARTICIPANTS

Le législateur confie la mission d'intégrateur de services fédéral au Service Public Fédéral Technologie de l'Information et de la Communication, dénommé « SPF Fedict »[13]. Ce SPF a été créé en 2001, pour assurer le développement des outils et services d'e-gouvernement dans l'administration fédérale. Il est notamment chargé « de développer une stratégie commune en matière d'E-Government (…) et d'assister les services publics fédéraux lors de la mise en œuvre de cette stratégie commune »[14].

Les administrations qui bénéficient des prestations de l'intégrateur de services fédéral et/ou qui lui fournissent des données sont qualifiées de « services publics participants »[15]. Tous les services publics fédéraux sont visés par cette notion, à l'exception du SPF Fedict lui-même et des services publics fédéraux qui font déjà partie du réseau sectoriel de la sécurité sociale et du réseau sectoriel santé[16].

C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, « L'application de la Convention 108 au mécanisme de profilage. Éléments de réflexion destinés au travail futur du Comité consultatif », mars 2008, T-PD (2008) 01, p. 5 ; E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n° 40 et s.

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

[10] *M.B.*, 29 août 2012. Ci-après « loi du 15 août 2012 ».

[11] À ce sujet, voy. *infra,* II, n° 2.

[12] À ce sujet, voy. not. Cour eur. D.H., *Rotaru c. Roumanie*, 4 mai 2000, § 43 ; Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in *État de droit et virtualité* (dir. K. BENYEKHLEF et P. TRUDEL), Montréal, Thémis, 2009, pp. 169 et s. ; E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, n^{os} 59 et s.

[13] Article 3 de la loi du 15 août 2012.

[14] Article 2 de l'arrêté royal du 11 mai 2001 portant création du Service public fédéral Technologie de l'Information et de la Communication.

[15] Article 2, 10°, de la loi du 15 août 2012.

[16] Plus précisément, l'article 2, 10°, alinéa 2, de la loi du 15 août 2012 indique que « ne sont pas des services participants :

De plus, « toute instance ou tout service, doté ou non de la personnalité juridique, qui dépend de l'administration fédérale »[17], est également considéré comme un service public participant dès le moment où il participe au réseau en mettant des données à disposition de l'intégrateur de services fédéral ou en collectant des données via celui-ci. Lors des discussions parlementaires précédent l'adoption de la loi du 15 août 2012, le législateur a précisé qu'il s'agit des instances et services sur lesquels « l'État belge exerce une compétence en termes de financement, d'administration ou de contrôle »[18].

Enfin, peut également être qualifié de service public participant, une personne ou une instance désignée par le Roi, en prenant un arrêté délibéré en Conseil des Ministres après avoir recueilli l'avis de la Commission de la protection de la vie privée, notamment[19]. Cette dernière a d'ailleurs insisté sur le fait que, pour ne pas mettre en péril la vie privée des citoyens, on ne peut admettre qu'une entreprise purement commerciale soit désignée par le Roi comme une instance participant au fonctionnement de l'intégrateur de services fédéral. En effet, « par la nature de sa tâche, des masses de données à caractère personnel, parmi lesquelles aussi parfois des données sensibles, [sont] transmises par l'intégrateur. Ces données ont aussi une valeur commerciale. Le risque que les intérêts commerciaux prévalent par rapport à la tâche d'intérêt général est donc un risque bien réel avec toutes les conséquences qui peuvent en découler »[20].

Pour faciliter la clarté de l'exposé, les institutions qui participent au fonctionnement de l'intégrateur de services fédéral sont qualifiées d'« administrations du réseau fédéral » dans les lignes qui suivent.

a) les services publics fédéraux en charge de la Sécurité sociale, de la Santé publique, de la Sécurité de la Chaîne alimentaire, de l'Environnement, de l'Emploi, du Travail et de la Concertation sociale, ainsi que les services publics de programmation dépendant de ces services publics fédéraux ;
b) les institutions publiques de sécurité sociale au sens de l'arrêté royal portant des mesures en vue de la responsabilisation des institutions publiques de sécurité sociale, en application de l'article 47 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions, les institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, ainsi que les institutions auxquelles certains droits et obligations ont été étendus en vertu de l'article 18 de la loi précitée du 15 janvier 1990 ;
c) l'intégrateur de services fédéral ».

[17] Article 2, 10°, de la loi du 15 août 2012.

[18] Projet de loi relatif à la création et à l'organisation d'un intégrateur de services fédéral, Exposé des motifs, *Doc. parl.*, Ch. Repr., session 2011-2012, n° 53-2223/001, p. 19.

[19] Article 2, 10° et article 46 de la loi du 15 août 2012.

[20] CPVP, avis n° 41/2008 précité, n° 19.

3. Les sources authentiques de données

Parmi les services publics participants, certains sont responsables d'une source authentique de données.

a) La notion

La « source authentique de données » fait partie des notions nouvelles auxquelles sont aujourd'hui confrontées les administrations. La loi du 15 août 2012 la définit comme une « banque de données dans laquelle sont conservées des données authentiques », une donnée authentique étant une « donnée récoltée et gérée par une instance dans une base de données et qui fait foi comme donnée unique et originale concernant la personne ou le fait de droit concerné, de sorte que d'autres instances ne doivent plus collecter cette même donnée ».

Pour le dire autrement, dans la loi du 15 août 2012, le qualificatif « authentique » n'a pas la même signification que celle qu'il peut avoir notamment dans le Code civil lorsqu'il régit la preuve par « titre authentique », par exemple[21]. Dans le contexte de l'e-gouvernement en général, et dans la loi du 15 août 2012 en particulier, une « source authentique de données » est une base de données contenant des informations relatives à une personne physique ou morale qui ont une valeur unique dans l'administration en raison du fait que leur collecte, leur enregistrement, leur mise à jour et leur destruction sont assurés exclusivement par une administration déterminée. En outre, les données contenues dans la source authentique de données sont destinées à être réutilisées par les autres administrations du réseau, grâce à l'intégrateur de services qui assure l'échange de ces données entre ces administrations[22].

b) La raison d'être

La mise en place de sources authentiques de données s'explique par la volonté actuelle du législateur d'organiser une réutilisation maximale des données détenues par les administrations, dans le but de ne pas demander de multiples fois les mêmes informations aux citoyens et de gagner ainsi du temps et de l'argent[23]. Pour satisfaire à cet objectif, les informations réutilisées doivent être fiables, c'est-à-dire correctes et à jour. Si tel n'était pas le cas, l'erreur affectant la donnée réu-

[21] Articles 1317 et s. du Code civil.

[22] À ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, nos 13 et s. et références citées.

[23] Voy. *infra,* III, n° 2.

tilisée serait démultipliée autant de fois qu'il y a eu de réutilisations de cette donnée. C'est pourquoi, une fois la donnée collectée, il est important qu'elle soit enregistrée à un seul endroit – la source authentique de données – qui est placée sous la responsabilité d'une seule administration. Cette dernière doit ensuite assurer la fiabilité des données de la source authentique de données, de manière à ce que d'autres administrations puissent les réutiliser en toute confiance.

c) L'exemple du Registre national

Le Registre national des personnes physiques, régi par la loi du 8 août 1983 organisant un registre national des personnes physiques[24], est une source authentique de données[25], qui contient les données d'identification des citoyens.

Les treize informations d'identification enregistrées au Registre national sont reprises à l'article 3 de la loi sur le Registre national. Il s'agit notamment des nom et prénoms, de l'adresse, de l'état civil, du sexe, de toutes les personnes physiques inscrites dans certains registres « papiers » disséminés dans tout le pays, à savoir, les registres de la population et les registres des étrangers tenus dans les communes[26], les registres tenus dans les missions diplomatiques et les postes consulaires belges à l'étranger[27], et les registres d'attente tenus par les communes où sont inscrits les étrangers qui se déclarent réfugiés ou qui demandent la reconnaissance de la qualité de réfugié[28].

Ces informations ont une valeur unique dans l'administration, ce qui signifie qu'en principe[29], elles ne sont enregistrées qu'au Registre national.

d) La désignation des administrations fédérales détenant une source authentique de données

Le législateur a délégué au Roi le soin de répartir les sources authentiques de données parmi les administrations du réseau fédéral. Il doit le faire par un arrêté royal délibéré en Conseil des ministres. Cette tâche dévolue au Roi est appelée « répartition fonctionnelle »[30]. Le Roi effectue cette répartition sur la base de propositions formulées par le comité de coordination de Fedict, éventuellement après avoir recueilli l'avis de la Commission de la protection de la vie privée pour les sources authentiques contenant des données à caractère personnel. Ces propositions contiennent les critères sur la base desquels des données sont qualifiées d'authentiques ainsi que l'identification de données qui, au sein du réseau fédéral, peuvent être qualifiées d'authentiques[31].

Par exemple, au sein du réseau fédéral, le SPF Intérieur est l'administration responsable de la source authentique « Registre national »[32].

Pour l'heure, les arrêtés royaux déterminant les critères d'une source authentique de données ainsi que la liste des données authentiques disponibles au niveau fédéral sont en cours de rédaction.

e) La responsabilité d'une administration détentrice d'une source authentique de données

L'administration responsable d'une source authentique de données est soumise à une obligation de fiabilité des données et à une obligation de collaboration avec l'intégrateur de services fédéral[33].

L'obligation de fiabilité des données signifie que l'administration qui détient une source authentique est responsable de la qualité des données qui s'y trouvent. Elle doit tout mettre en œuvre pour garantir que les données émises sont exactes et à jour afin d'éviter que des données erronées circulent au sein du réseau fédéral. C'est ce qui explique que l'Office national des pensions, par exemple, envoie à intervalles réguliers, aux personnes reprises dans la source authentique de données qu'elle détient, un inventaire des données reprises à leur sujet en leur demandant de vérifier l'exactitude de ces informations.

Corollairement à l'obligation de garantir la fiabilité des données, la Commission de la protection de la vie privée suggère de mettre en place certaines garanties procédurales entourant la qualité

[24] *M.B.*, 21 avril 1984. Ci-après « loi sur le Registre national ».

[25] Projet de loi relatif à la création et à l'organisation d'un intégrateur de services fédéral, Exposé des motifs, *Doc. parl.*, Ch. Repr., session 2011-2012, n° 53-2223/001, précité, p. 18 ; CPVP, avis n° 14/2005 du 28 septembre 2005, du 28 septembre 2005 faisant suite à une décision d'évocation dans les dossiers SCSZ/05/70, SCSZ/05/90, SCS/05/110 et SCSZ/05/113 transmise par le Président du Comité sectoriel de la Sécurité sociale, p. 3 ; CPVP, recommandation n° 09/2012 du 23 mai 2012 relative aux sources authentiques de données dans le secteur public, p. 3, note 7.

[26] Le registre de la population contient les données relatives aux Belges, tandis que le registre des étrangers contient les données relatives aux étrangers admis ou autorisés à s'établir ou à séjourner dans le Royaume [Projet de loi créant un registre d'attente pour les étrangers qui se déclarent réfugiés ou qui demandent la reconnaissance de la qualité de réfugié. Rapport fait au nom de la Commission de l'intérieur par M. Cannaerts, *Doc. parl.*, Sénat, sess. ord. 1993-1994, n° 1015-2, p. 2]. Ces deux types de registres sont généralement regroupés sous le vocable générique de registres de la population, comme le prévoit l'article 1er de la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité.

[27] Même si la loi ne le précise pas, dans ce cas, seuls les ressortissants belges sont enregistrés au Registre national [Rapport au Roi précédant l'arrêté royal du 3 avril 1984 relatif à l'accès de certaines autorités publiques au Registre national des personnes physiques, ainsi qu'à la tenue à jour et au contrôle des informations, *M.B.,* 21 avril 1984, également publié dans *Pasin.*, 1984, p. 687].

[28] Article 2, alinéa 1er, de la loi.

[29] Nous nuançons notre propos dans la mesure où, pour l'heure, de nombreux duplicata des données d'identification des citoyens existent dans les administrations. Cela tient au fait que la mise en place de sources authentiques de données est relativement récente, ce qui devrait changer progressivement.

[30] Article 6 de la loi du 15 août 2012.

[31] Article 27, § 2, de la loi du 15 août 2012.

[32] CPVP, avis n° 14/2005 du 28 septembre 2005, *op. cit.*, p. 3.

[33] Article 6 de la loi du 15 août 2012.

des données de la source authentique. Il peut ainsi être judicieux que l'administration responsable de la source authentique enregistre les modifications apportées aux données. Ce faisant, on peut savoir, par exemple, à partir de quand la donnée a été mise à jour et rectifier les éventuelles communications de données qui n'en auraient pas tenu compte. Il y a lieu également d'imposer aux administrations de conserver l'historique de l'accès aux données et de mettre en place un « contrôle de la qualité à l'égard des utilisateurs », c'est-à-dire, un système qui avertit les utilisateurs qu'une donnée communiquée était fautive et a été depuis corrigée[34].

Quant à *l'obligation de collaboration* imposée à l'administration responsable d'une source authentique de données, elle signifie que ladite administration est contrainte de fournir à l'intégrateur de services les données dont elle assure l'enregistrement lorsque l'intégrateur de services les lui réclame, sous peine de bloquer le fonctionnement du réseau.

III. L'ACCÈS AUX DONNÉES VIA L'INTÉGRATEUR DE SERVICES FÉDÉRAL

1. Le rôle de Fedict

Une administration fédérale peut s'adresser à Fedict dans le but d'obtenir des données à caractère personnel[35] relatives à un citoyen dont elle gère le dossier. Elle peut également le faire pour accéder à des données qui n'ont pas un caractère personnel, telles que des données relatives aux entreprises[36]. Concrètement, pour l'heure, seules les données de la source authentique « Registre national » et « Registre *bis* »[37] ainsi que les données de la source authentique « Banque-carrefour des entreprises » sont accessibles via Fedict. Néanmoins, à terme, les données accessibles via Fedict devraient être bien plus nombreuses.

Une fois saisi d'une demande d'une administration, Fedict entame la recherche de données au sein du réseau fédéral. Pour ce faire, il identifie, au sein du réseau fédéral, la source authentique de données qui contient les informations recherchées. Ainsi par exemple, les données relatives aux coordonnées des contribuables sont enregistrées au Registre national, source authentique de données placée sous la responsabilité du SPF Intérieur.

Fedict demande ensuite à l'administration responsable de cette source authentique de données de lui fournir les informations recherchées. Ainsi qu'on l'a dit[38], l'administration est légalement obligée de répondre positivement à cette demande[39].

L'intégrateur de services est alors amené à accomplir des tâches distinctes selon les besoins de l'administration demanderesse des données : soit il communique les données sans les intégrer, soit il procède à une intégration de données avant de communiquer celles-ci.

Plus précisément, si une administration du réseau n'a besoin que de prendre connaissance de données provenant d'une seule base de données, le rôle de l'intégrateur de services se réduit à communiquer lesdites informations. Par exemple, le SPF Finances a besoin des coordonnées des contribuables. Fedict se contente de lui fournir ces données qui émanent du Registre national.

Une administration peut également avoir besoin d'informations qui sont le résultat d'une mise en relation de plusieurs types de données. Dans ce cas, l'intégrateur de services effectuera lui-même cette mise en relation des données, appelée « intégration de données ». Par exemple, aujourd'hui, les personnes se trouvant dans une situation financière précaire peuvent obtenir automatiquement une réduction tarifaire pour la fourniture de gaz naturel et d'électricité[40]. Cette automatisation est rendue possible par un croisement entre différentes bases de données, qu'effectue l'intégrateur de services. Concrètement, les fournisseurs d'énergie communiquent au SPF Économie le nom de leurs clients. Le SPF Économie s'adresse ensuite

[34] CPVP, avis n° 11/2009, du 29 avril 2009 concernant le projet d'arrêté du Gouvernement flamand portant exécution du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, p. 3, n° 9.

[35] Une donnée à caractère personnel consiste en « toute information concernant une personne identifiée ou identifiable » (voy. not. l'article 2, a) de la 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 ; article 1er, 6 1er, 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). La notion est donc large et vise aussi bien le numéro d'identification au Registre national, qu'un numéro de plaque d'immatriculation, des photos, un numéro de compte bancaire, etc. À ce sujet, voy. not. H. Graux et J. Dumortier, *Privacywetgeving in de praktijk*, Courtrai, UGA, 2009, pp. 22 et 32 ; C. de Terwangne, « La nouvelle loi belge de protection des données à caractère personnel », in *Cahiers de sciences morales et politiques,* 2002, p. 92.

[36] À ce sujet, voy., sur le site internet de Fedict, http://www.fedict.belgium.be/fr/echange_de_donnees/donnees_a_caractere_personnel/.

[37] Certaines personnes ne sont pas enregistrées au Registre national mais sont néanmoins amenées à être en contact avec des administrations belges, telles que les administrations de sécurité sociale. C'est le cas, par exemple, des personnes vivant à l'étranger mais travaillant en Belgique. Les données d'identification de ces personnes sont enregistrées dans une base de données détenue par la Banque-carrefour de la sécurité sociale, qui fait office de source d'identification complémentaire au Registre national et appelée « Registre *bis* ». Ces personnes sont identifiées au sein de l'Administration à l'aide de leur numéro d'identification de la Banque-carrefour de la sécurité sociale, dit aussi « numéro *bis* » [article 8, 2°, de la loi du 15 janvier 1990].

[38] Voy. *supra*, II, n° 3.

[39] L'article 6 de la loi du 15 août 2012 affirme que « les instances chargées du stockage des données authentiques sont dans l'obligation de (…) rendre accessibles par le biais du réseau les données dont l'enregistrement leur est confié ».

[40] Articles 3 et s. de la loi-programme du 27 avril 2007, *M.B.*, 8 mai 2007.

à l'intégrateur de services[41] pour savoir qui, parmi ces clients, a droit au tarif social et doit donc être considéré comme un « client protégé ». L'intégrateur de services contacte alors le SPF Finances pour connaître le montant du revenu des citoyens qui achètent du gaz et de l'électricité. Il identifie ensuite lui-même, parmi ces clients, ceux dont le revenu ne dépasse pas le seuil en dessous duquel ils ont droit au tarif social. Cette opération de mise en relation entre les données communiquées par le SPF Finances, les données communiquées par le SPF Économie, et la confrontation au seuil de revenu est appelée « intégration de données », qui se distingue donc d'une simple « consultation » de données. Finalement, l'intégrateur de services communique au SPF Économie l'identité des seuls clients protégés et non le montant exact du revenu de tous les clients des fournisseurs de gaz et d'électricité. De cette manière, la tâche du SPF Économie est facilitée, puisque ce dernier reçoit de l'intégrateur de services la liste des clients protégés, sans devoir les identifier lui-même parmi l'ensemble des clients. De plus, cette mesure protège la vie privée des citoyens puisque le SPF Économie ne connaît pas leur revenu exact et dispose uniquement de l'information dont il a besoin, à savoir si oui ou non ces clients ont droit au tarif social.

2. L'objectif de la collecte unique des données

Ainsi donc, le fait de confier à Fedict la mission d'intégrateur de services fédéral doit permettre une réutilisation maximale des informations qui sont déjà détenues au sein des administrations fédérales. L'idée est de faire en sorte que le citoyen ne doive communiquer ses données à caractère personnel qu'une seule fois aux administrations du réseau fédéral et que, dès qu'une institution a besoin d'une de ces informations, elle s'adresse à Fedict plutôt qu'au citoyen.

Cet objectif de la collecte unique des données, dit aussi « *only once* », a été façonné en réaction aux vicissitudes de l'administration en silos évoquée précédemment. A l'époque, les citoyens étaient contraints de fournir la même information de multiples fois à toutes les administrations qui en avaient besoin, puisque chacune de ces institutions travaillait séparément pour accomplir ses propres missions. Il en résultait une perte de temps et d'argent, tant pour le citoyen que pour l'administration, et ce d'autant plus que la répétition des mêmes informations générait souvent des erreurs dans l'encodage des données et la transmission de celles-ci.

Deux questions particulières retiennent l'attention à ce stade. Les administrations sont-elles obligées de faire appel à Fedict pour accéder à des données ? Par ailleurs, comment savoir quelles données sont disponibles dans le réseau fédéral ?

A. La collecte indirecte des données

3. Une obligation légale très récente

Le fait, pour les administrations fédérales, de s'adresser à Fedict pour obtenir des données disponibles dans le réseau – ce que l'on appelle la collecte indirecte de données – plutôt que de demander ces informations directement à la personne concernée – ce que l'on appelle la collecte directe des données – était, pendant plusieurs années, une possibilité laissée à la discrétion des administrations fédérales.

Depuis peu, ces administrations n'ont plus le choix. Une loi du 5 mai 2014[42] ajoute, dans la loi du 15 août 2012, l'obligation, pour les administrations du réseau fédéral, de collecter les données disponibles dans ce réseau auprès de Fedict et non plus auprès des personnes concernées.

Ainsi, l'article 8 de la loi du 15 août 2012 est complété comme suit « § 3. Les services publics participants collectent (…) les données électroniques disponibles qui sont offertes par l'intégrateur de services fédéral auprès de ce dernier.

Les services publics participants ne recueillent plus les données dont ils disposent en exécution de l'alinéa 1er auprès de l'intéressé (…) ».

En d'autres termes, dès lors que les données recherchées sont disponibles dans le réseau fédéral, les administrations de ce réseau ne peuvent plus s'adresser aux personnes concernées pour les obtenir. Elles doivent se tourner exclusivement vers Fedict[43].

Concrètement, cela signifie que ces administrations ne peuvent plus demander aux citoyens et aux entreprises des documents qu'elles sont en mesure d'obtenir en s'adressant à Fedict. De plus, elles ne

[41] Actuellement, la mission d'intégrateur de services dans ce domaine est confiée à la Banque-carrefour de la sécurité sociale mais pourrait, à plus long terme, être confiée à Fedict. À ce sujet, voy. la délibération du Comité sectoriel pour l'Autorité fédérale n° 10/2009 du 9 juillet 2009 relative à la transmission de données à caractère personnel du SPF Finances au SPF Économie, PME, Classes moyennes et Énergie, via la Banque-carrefour de la Sécurité sociale, en vue de l'octroi d'une réduction forfaitaire pour la fourniture de gaz naturel, d'électricité et de mazout, n° 6.

[42] Loi du 5 mai 2014 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, *M.B.*, 4 juin 2014. L'article 13 de cette loi impose la collecte indirecte des données par l'ajout de 2 paragraphes à l'article 8 de la loi du 15 août 2012.

[43] Article 8, § 13, de la loi du 15 août 2012 telle que modifiée par la loi du 5 mai 2014 précitée.

peuvent plus exiger du citoyen et des entreprises qu'ils avertissent chaque administration d'une mise à jour de leurs informations si cette mise à jour est disponible dans une source authentique du réseau fédéral et accessible via Fedict.

Cette obligation nouvelle imposée aux administrations du réseau fédéral s'inspire directement de l'obligation de collecte indirecte ancrée depuis quelques années dans d'autres législations particulières. En effet, cette obligation est déjà imposée aux administrations pour les données accessibles via la Banque-carrefour de la sécurité sociale[44] ainsi que les données contenues dans le Registre national[45], dans la Banque-carrefour des entreprises[46] et dans la Banque-carrefour des véhicules[47].

La loi précitée du 5 mai 2014 étend l'obligation de collecte indirecte des données à l'ensemble des administrations du réseau fédéral en se fondant sur le constat qu'« en pratique les services publics n'utilisent pas toujours les données disponibles dans les sources authentiques et continuent de réclamer les données en question auprès des intéressés (…). Par ailleurs, il se basent souvent sur des réglementations internes contradictoires qui prévoient expressément que les informations doivent être réclamées auprès des citoyens ou des entreprises ou que ces derniers sont tenus de leur communiquer toute information utile »[48].

4. Les conséquences du non-respect de l'obligation de collecte indirecte

À l'avenir, le non-respect de l'obligation de collecte indirecte des données emportera des conséquences non négligeables.

En effet, si une administration du réseau fédéral collecte directement auprès du citoyen ou d'une entreprise une information qu'elle aurait dû obtenir via l'intégrateur de services fédéral Fedict, elle agit en violation de l'article 8 de la loi du 15 août 2012. On doit alors considérer que les données relatives aux personnes ou entreprises concernées ont été obtenues illégalement, ce qui vicie la décision administrative prise sur la base de ces données. Dans le même sens, une administration ne peut plus refuser l'octroi d'un droit à un citoyen ou à une entreprise au seul motif qu'il ne lui a pas communiqué une information nécessaire, si celle-ci est disponible dans le réseau fédéral et que ladite administration peut y accéder via Fedict.

5. Illustrations jurisprudentielles dans le secteur de la sécurité sociale

Pour l'heure, l'obligation de collecte indirecte des données dans le réseau fédéral est trop récente pour que les cours et tribunaux aient déjà pu se prononcer sur les conséquences du non-respect de cette obligation. Néanmoins, rappelons qu'une obligation de collecte indirecte identique à celle organisée par la loi du 5 mai 2014 est consacrée depuis plusieurs années par l'article 11 de la loi relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, et s'impose aux institutions de sécurité sociale pour les données disponibles dans le réseau de la sécurité sociale et accessibles via la Banque-carrefour de la sécurité sociale. Dans ce domaine, des décisions judiciaires existent, qui sanctionnent le non-respect de cette obligation. Elles sont encore rares mais s'avèrent particulièrement pertinentes.

Ainsi, par exemple, un arrêt rendu par la Cour du travail de Bruxelles, le 21 avril 2010[49], illustre le fait que l'obligation de collecte indirecte aboutit à contraindre les institutions de sécurité sociale à trouver par elles-mêmes les documents dont elles ont besoin dans l'exécution de leurs missions. C'est particulièrement intéressant, par exemple, pour un demandeur du revenu d'intégration sociale à qui le CPAS réclamerait un document que ce demandeur n'est pas en mesure de fournir alors que les informations recherchées sont disponibles dans le réseau de la sécurité sociale et que le CPAS peut y accéder. Dans un tel cas, malgré le fait qu'il n'a pas fourni ledit document, ce demandeur d'allocation ne peut pas se voir reprocher un manque de collaboration au sens de l'article 19, § 2, de la loi concernant le droit à l'intégration sociale[50] qui amènerait le CPAS à refuser l'octroi du revenu d'intégration sociale à cet assuré social. Le CPAS a, en effet, l'obligation de recueillir d'initiative les documents accessibles via la Banque-carrefour de la sécurité sociale[51].

[44] Article 11 de la loi du 15 janvier 1990 relative la Banque-carrefour de la sécurité sociale.

[45] Article 6 de la loi du 8 août 1983 sur le Registre national.

[46] Article 22 de la loi du 16 janvier 2003 portant création d'une Banque-carrefour des Entreprises. Contrairement à ce que son nom laisse à penser, la Banque-carrefour des entreprises est une source authentique de données. À ce sujet voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, n° 20 et références citées.

[47] Article 23 de la loi du 19 mai 2010 portant création de la Banque-carrefour des véhicules. Comme la Banque-carrefour des Entreprises, la Banque-carrefour des véhicules est, en partie du moins, une source authentique de données. Voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n° 14 et références citées.

[48] Projet de loi ancrant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour les autorités publiques et portant simplification et assimilation des formulaires électroniques et papier, *op. cit.*, n° 53-3387/001, p. 6.

[49] C. trav. Bruxelles (8e ch.), 21 avril 2010, R.G. n° 2008/AB/51591 et n° 2009/AB/51809.

[50] Loi du 26 mai 2002 concernant le droit à l'intégration sociale, *M.B.*, 31 mai 2002.

[51] C. trav. Bruxelles (8e ch.), 21 avril 2010, *op. cit.*, 6e feuillet.

D'autres décisions judiciaires rappellent que, par application de l'obligation de collecte indirecte des données, les institutions de sécurité sociale doivent veiller elles-mêmes à utiliser des données à jour, dès le moment où celles-ci sont disponibles dans le réseau de la sécurité sociale. La Cour du travail de Liège, par exemple, a rendu un arrêt à ce sujet le 27 juin 2006, en matière de droit à la pension[52]. Dans cette affaire, l'Office national des pensions[53] reproche à un homme pensionné de ne pas l'avoir averti du décès de son épouse, ce qui a des conséquences au niveau du montant de la pension qui lui est due. L'O.N.P. souhaitait récupérer le montant de pension trop élevé qu'elle avait payé durant cinq ans, en invoquant les règles de prescription applicables en cas de mauvaise foi de l'assuré. Or, il s'avère que l'assuré social avait averti la commune du décès de son épouse. Cette information était donc enregistrée au Registre national, qui fait partie du réseau de la sécurité sociale. L'O.N.P., lui aussi inclus dans le réseau de la sécurité sociale, avait donc accès à cette information 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'O.N.P. 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 »[54].

En d'autres termes, dès le moment où l'assuré social communique à sa commune la mise à jour d'une information enregistrée au Registre national, il n'est plus contraint d'avertir les institutions de sécurité sociale de ce changement. C'est à ces dernières qu'il revient de mettre à jour les informations sur lesquelles elles fondent leurs prestations et ce d'autant plus que, le plus souvent, ces mises à jour leur parviennent automatiquement.

Remarquons que, une fois l'obligation de collecte indirecte imposée à l'ensemble des administrations du réseau fédéral, la même solution sera applicable à celles-ci puisque les informations du Registre national sont accessibles via Fedict.

[52] C. trav. Liège, 27 juin 2006, *J.L.M.B.*, 2007, pp. 1043-1047.
[53] Ci-après « O.N.P. ».
[54] C. trav. Liège, 27 juin 2006, *op. cit.*, p. 1047.

6. Une nécessaire et légitime modification des habitudes administratives

L'obligation de collecte indirecte des données contraint les administrations à utiliser les outils technologiques à leur disposition et, ce faisant, à modifier leurs habitudes. Un parlementaire s'est d'ailleurs prononcé clairement en ce sens lors des discussions préparatoires au récent projet de loi précité, affirmant que « pour concrétiser les objectifs du projet de loi, un changement de mentalité est nécessaire de la part des administrations. Redemander constamment des attestations aux citoyens et aux entreprises est une pratique courante. Cette méthode devra céder la place à une volonté de prendre soi-même l'initiative d'aller chercher les données nécessaires auprès des sources authentiques »[55]. À défaut de le faire, l'administration risquerait d'adopter des décisions illégales qui ne pourraient être appliquées.

À notre sens, l'obligation de collecte indirecte et la responsabilisation des administrations qui s'en suit est légitime. Elle répond à une volonté forte du législateur, affirmée dès les années nonante déjà[56], que la simplification administrative bénéficie tant aux administrations qu'aux citoyens et aux entreprises. Tous doivent gagner en confort grâce à l'informatisation des tâches administratives.

Dans le même temps, l'obligation de collecte indirecte des données et les sanctions applicables en cas de non-respect de celle-ci répondent à un but légitime dans notre société démocratique, celui de veiller à un certain équilibre entre l'administration et le citoyen[57]. En effet, grâce à l'intégrateur de services, l'administration gagne en efficacité et en confort dans l'accomplissement de son travail. Cela se fait en contraignant le citoyen à accepter que l'administration s'ingère à de multiples reprises dans sa vie privée en traitant ses données à caractère personnel. Il est légitime que ce citoyen ait un retour bénéfique direct du système mis en place, afin d'assurer une réciprocité des

[55] Intervention de Peter Vanvelthoven, Projet de loi 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 papiers, *op. cit.*, n° 53-3387/004, p. 7.
[56] Entre autres exemples, voy. les travaux préparatoires de la loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale, en particulier l'exposé des motifs, *Pasin.*, Ch. Repr., session 1988-1989, n° 899/1, p. 77 : « la première mission de la Banque-carrefour (la transformation des flux d'informations actuels, désordonnés et éparpillés sur support papier, en flux électroniques coordonnés et harmonisés) doit permettre de réduire pour les personnes physiques et morales intéressées les charges ou obligations, le travail découlant d'une collecte de données qui est loin d'être caractérisée par l'unicité, de réduire les coûts administratifs de fonctionnement, les coûts sociaux dus aux cumuls indus non dépistés et d'accélérer le service rendu ».
[57] Pour de plus amples développements à ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^{os} 47 à 49.

avantages de la technologie entre l'administration et le citoyen[58].

B. L'identification des données disponibles dans le réseau fédéral

7. La transparence du réseau fédéral

Ainsi donc, depuis peu, les administrations ne peuvent plus demander aux citoyens et aux entreprises les données auxquelles elles peuvent avoir accès via Fedict. De leur côté, les citoyens et les entreprises ne doivent plus se soucier de fournir ces informations et leur mise à jour à chaque administration du réseau fédéral, dès le moment où ces informations sont déjà enregistrées dans l'une des sources authentiques du réseau. Par ailleurs, les cours et tribunaux vont devoir tirer les conséquences juridiques, dans chaque cas d'espèce, du non-respect, par les administrations du réseau fédéral, de l'obligation de collecter indirectement lesdites données.

C'est pourquoi, il importe que chacun puisse connaître, aisément et avec précision, les types de données disponibles dans le réseau fédéral et accessibles via Fedict afin de pouvoir affirmer avec certitude que, pour ces types de données, les administrations du réseau fédéral sont soumises à l'obligation de collecte indirecte.

Pour atteindre cet objectif, un rigoureux travail de transparence doit être réalisé, qui permette d'assurer la publicité des sources authentiques de données du réseau fédéral et des types de données qui y sont enregistrés. À notre sens, cette mission revient à Fedict, en tant qu'intégrateur de services fédéral. En effet, Fedict a connaissance des sources authentiques de données se trouvant dans le réseau fédéral et des types de données qui y sont enregistrés. Sans cela, il ne serait pas en mesure d'acheminer les informations vers les administrations qui les ont demandées. De plus, cette tâche entre pleinement dans les missions qui lui ont été attribuées et qui consistent notamment à « développer une stratégie commune en matière d'E-Government (…) [et] développer les normes, les standards et l'architecture de base nécessaires pour une mise en oeuvre efficace de la technologie de l'information et de la communication à l'appui de cette stratégie »[59].

8. Des justifications constitutionnelles et légales

Le travail de transparence qui devrait être effectué par Fedict se justifie pour deux raisons principalement.

Il s'agit, tout d'abord, d'une mesure de protection de la *vie privée* des citoyens. Le droit fondamental à la vie privée, consacré par l'article 22 de la Constitution, s'entend aujourd'hui d'un droit à l'autodétermination informationnelle. En d'autres termes, chacun a le droit de décider lui-même de l'utilisation de ses données à caractère personnel ou, au moins[60], d'avoir connaissance de l'usage qui en est fait[61]. C'est pourquoi, en l'occurrence, il importe que chaque citoyen puisse avoir une vision claire des bases de données dans lesquelles sont et seront enregistrées les informations qu'il est contraint de donner à l'administration. Dans le même temps, le respect de cet impératif favorise la confiance du citoyen en l'État. Le fait de savoir ce que l'État détient comme données et par quelle administration ces données sont conservées apaise, d'une part, les peurs liées à l'existence d'un État « *Big brother* », qui saurait tout de tout le monde et, d'autre part, les craintes que l'usage des technologies dans le secteur public provoque le développement d'une administration kafkaïenne, c'est-à-dire une administration à ce point opaque et complexe qu'on ne parvient plus à la comprendre et la contrôler[62].

En outre, la mise en lumière des données enregistrées au sein du réseau fédéral se justifie au regard du droit fondamental à la *transparence administrative*, consacré par l'article 32 de la Constitution et organisé, au niveau fédéral, par loi du 11 avril 1994 relative à la publicité de l'administration[63]. Cette dernière impose à l'administration des obligations de publicité active qui

[58] Au sujet du principe de la réciprocité des avantages et de ses fondements, voy. *ibidem*, n^os^ 382 et 383.

[59] Article 2 de l'arrêté royal du 11 mai 2001 portant création du Service public fédéral Technologie de l'Information et de la Communication.

[60] Cette nuance est liée au fait que, dans l'e-gouvernement notamment, il y a des situations dans lesquelles le citoyen est obligé de donner ses informations personnelles. C'est le cas, par exemple, des données du Registre national qui sont obligatoirement communiquées et enregistrées à défaut de quoi, le citoyen n'aurait pas d'existence civile.

[61] Dans le même sens, voy. Y. Poullet, « L'informatique menace-t-elle nos libertés ? », in *La télématique*, *T. 1 : Aspects juridiques, techniques et socio-politiques. Actes du colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit (CRID) des Facultés Notre-Dame de Namur*, Gand, Story-Scientia, 1984, pp. 195 et 196 ; H. Burkert, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *Droit de l'informatiques et des Télécoms*, 1985, pp. 8 à 16 ; Th. Leonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in *La vie privée : une liberté parmi les autres ?* (dir. F. Rigaux), Bruxelles, Larcier, 1992, pp. 231 et s ; R. Leenes et B.-J. Koops, « "Code" and privacy or how technology is slowly eroding privacy », in *Coding regulation. Essays on the Normative Role of Information technology* (dir. E. Dommering et L. Asscher), La Haye, TMC Asser Press, 2006, pp. 143 et 144.

[62] Au sujet de ces craintes, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.,* n^os^ 61 et s.

[63] Loi du 11 avril 1994 relative à la publicité de l'administration, *M.B.*, 30 juin 1994.

consistent à fournir, d'initiative, « une information claire et objective sur l'action des autorités administratives fédérales »[64]. Dans le contexte de l'e-gouvernement et de l'administration structurée en réseaux, on peut raisonnablement considérer que toute personne doit pouvoir accéder à une vue d'ensemble de la localisation des données et de leur utilisation pour comprendre l'environnement administratif dans lequel elle se trouve. C'est d'autant plus aisé à mettre en place aujourd'hui que l'administration dispose de tous les outils technologiques permettant de créer un portail internet et d'y faire figurer les documents qu'elle souhaite[65]. En ce sens, la Charte des services publics impose d'ailleurs clairement aux services publics de recourir aux technologies pour s'adapter aux besoins du public, en affirmant que « par application de la loi du mutabilité, les services publics doivent s'efforcer de procurer un service adapté aux besoins des utilisateurs, comme aux techniques et moyens disponibles »[66].

9. Un panorama général du réseau

Pour l'heure, le site internet de Fedict ne présente que peu d'informations au sujet des types de données disponibles dans le réseau fédéral et celles-ci ne semblent pas aisément compréhensibles par tout un chacun.

En effet, en cliquant sur l'onglet « Échange de données », on accède à une rubrique « données à caractère personnel » indiquant que « les services web permettent de rechercher des données à caractère personnel dans le Registre national ou de rechercher et mettre à jour ce type de données dans le Registre *Bis* », ainsi qu'à une rubrique « données entreprises », précisant que « les services web permettent de créer, consulter et adapter des données d'entreprises et attestations dans les banques de données du SPF Économie ». Bien que ces indications soient utiles, elles ne sont pas suffisantes en ce que, notamment, elles n'énoncent pas les types de données enregistrés dans ces sources authentiques et n'indiquent pas l'administration responsable de chaque source authentique et de la fiabilité des informations qui y sont contenues[67].

Dès lors, il serait judicieux que Fedict crée un portail internet sur lequel figure un panorama des sources authentiques de données du réseau fédéral. En cliquant sur le nom de la source authentique de son choix, on devrait pouvoir visualiser les types de données qui y sont enregistrés ainsi que des informations utiles telles que l'administration responsable de cette base de données, la loi qui encadre cet enregistrement, etc.

IV. De nouvelles mesures à intégrer au sein des administrations du réseau fédéral

10. Des garanties de protection des données à caractère personnel

L'enregistrement de données à caractère personnel dans une source authentique de données, la communication de telles données à l'intégrateur de services fédéral, l'obtention de ces données de la part de l'intégrateur de services, sont autant de traitements de données à caractère personnel qui doivent être rigoureusement encadrés afin de répondre aux exigences de la protection de la vie privée et des données à caractère personnel des citoyens, consacrées notamment par l'article 22 de la Constitution, la directive européenne 95/46[68] et la loi du 8 décembre 1992[69] applicables en la matière.

C'est pourquoi, la loi du 15 août 2012 impose aux administrations concernées de respecter des règles particulières lors de l'utilisation des données à caractère personnel des citoyens. Les lignes qui suivent sont consacrées à trois mesures particulières que les administrations doivent mettre en place et qui sont liées à leur utilisation des données à caractère personnel des citoyens. Elles doivent engager un conseiller en sécurité, demander l'autorisation du comité sectoriel compétent pour chaque traitement de données à caractère personnel et répondre adéquatement aux droits d'accès et de rectification exercés par toute personne intéressée.

A. Désigner un conseiller en sécurité

11. La sécurité des données

L'intégrateur de services lui-même, ainsi que chaque administration du réseau fédéral, doivent désigner un conseiller en sécurité, au sein des membres de leur personnel ou en dehors[70]. Cette

[64] Article 2 de la loi du 11 avril 1994.

[65] Pour de plus amples détails à ce sujet, voy. not. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n[os] 377 et suivants.

[66] Charte de l'utilisateur des services publics du 4 décembre 1992, *M.B.*, 22 janvier 1993, Partie I, Chapitre II, Section 2.

[67] L'identification de l'administration responsable d'une source authentique importe notamment pour que le citoyen puisse exercer ses droits d'accès et de rectification des données qui le concernent. Voy. *infra,* n[os] 16 et s.

[68] 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.

[69] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

[70] Article 20 de la loi du 15 août 2012.

personne est chargée de veiller à la sécurité des données au sein de l'administration concernée, qu'il s'agisse de données à caractère personnel, ou non. Plus particulièrement, le conseiller en sécurité a une compétence d'avis et agit sous la responsabilité du fonctionnaire dirigeant de l'administration qui l'engage. Il est chargé, en somme, de proposer la mise en place de mesures de sécurité afin d'empêcher, par exemple, la fuite de données ou les « bugs » informatiques. En cas d'incident de sécurité, il analyse ces problèmes et suggère des solutions pour les résoudre et éviter qu'ils se reproduisent. Il est également le principal interlocuteur de l'administration pour toute question relative à la sécurité des données.

Bien que le conseiller en sécurité remplisse un rôle tout à fait nécessaire, il est regrettable que la loi n'impose pas que cette personne assume plutôt le rôle de détaché à la protection des données, ce qui répondrait à un souhait du législateur européen affirmé dans la directive 95/46[71]. D'ailleurs, plusieurs États européens imposent la présence d'un détaché à la protection des données au sein de leurs administrations[72]. Le rôle de détaché à la protection des données est plus large que celui de conseiller en sécurité. Non seulement, le détaché à la protection des données doit assurer la sécurité des données mais, étant également spécialisé en protection des données à caractère personnel, il doit veiller au respect des règles qui fondent cette matière. Cette personne est ainsi particulièrement indiquée, par exemple, pour répondre aux demandes d'accès aux données que tout citoyen peut adresser aux administrations[73].

Puisque chaque administration doit non seulement assurer la sécurité des données qu'elle utilise mais également satisfaire aux exigences de la protection des données à caractère personnel, on ne peut que leur conseiller d'engager un conseiller en sécurité apte à remplir également les tâches d'un détaché à la protection des données.

12. Le statut de conseiller en sécurité

Le statut de conseiller en sécurité est précisé dans un arrêté royal du 17 mars 2013[74]. Celui-ci fixe notamment un certain nombre de conditions pour pouvoir exercer cette fonction.

Ainsi, le conseiller en sécurité doit être en mesure de travailler de manière objective et impartiale. C'est la raison pour laquelle il ne pourrait pas exercer, complémentairement au rôle de conseiller en sécurité, une fonction incompatible avec celui-ci. Par exemple, le membre du service ICT d'une administration ne peut en principe pas être également conseiller en sécurité, au risque d'être simultanément contrôleur et contrôlé. Dans le même sens, pour assurer son indépendance vis-à-vis de ses supérieurs hiérarchiques notamment, l'arrêté royal prévoit que « le conseiller en sécurité et les collaborateurs éventuels ne peuvent pas être relevés de cette fonction en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent dans le cadre de l'exercice correct de leur fonction »[75].

Par ailleurs, le conseiller en sécurité doit faire preuve de compétences solides en informatique notamment, si bien qu'il est parfois amené à devoir suivre une formation spécialisée avant son entrée en fonction.

13. L'approbation de la Commission de la protection de la vie privée

La désignation du conseiller en sécurité doit être approuvée par la Commission de la protection de la vie privée, chargée de vérifier que la personne pressentie répond aux conditions légales et réglementaires entourant le statut de conseiller en sécurité. À cette fin, la Commission de la protection de la vie privée met à disposition des administrations un questionnaire d'évaluation pour le candidat conseiller en sécurité. Ce questionnaire est disponible sur le site internet de la Commission de la protection de la vie privée[76].

B. Obtenir l'autorisation du comité sectoriel compétent

14. Les comités sectoriels

Les comités sectoriels sont des organes de la Commission de la protection de la vie privée. Ils ont un pouvoir de décision, celui d'autoriser ou de refuser un traitement de données à caractère personnel, tel qu'un transfert de données entre deux

[71] Considérant 49 et article 18 de la directive 95/46.

[72] Par exemple, en Allemagne, la présence d'un détaché à la protection des données est obligatoire dans les organismes du secteur public, au niveau fédéral notamment (Article 4f (1) de la *Bundesdatenschutzgesetz*. Pour un commentaire de ce régime, voy. N. Métallinos, « La fonction de "détaché à la protection des données" en Allemagne et aux Pays-Bas », *Droit social*, n° 12, 2004, p. 1068). En Suisse, chaque institution fédérale doit également désigner un détaché à la protection des données (article 23 de l'Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993).

[73] À ce sujet, voy. *infra,* IV, C, n[os] 16 et s.

[74] Arrêté royal du 17 mars 2013 relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, *M.B.*, 22 mars 2013 (ci-après « arrêté royal du 17 mars 2013 »).

[75] Article 3 de l'arrêté royal du 17 mars 2013.

[76] Voy. http://www.privacycommission.be/fr/conseiller-en-securite-information Le questionnaire d'évaluation doit être renvoyé au comité sectoriel compétent institué au sein de la Commission de la protection de la vie privée, déterminé en fonction du type de données concerné.

administrations[77]. Il existe actuellement six comités sectoriels, chacun étant compétent en fonction de la nature des données qu'il contrôle.

Ainsi, le *Comité sectoriel du Registre national* est compétent pour octroyer « l'autorisation d'accéder aux informations [enregistrées dans le Registre national] »[78] ainsi que « l'autorisation d'utiliser le numéro d'identification du Registre national »[79].

Le *Comité sectoriel de la Banque-carrefour des Entreprises* est compétent pour autoriser l'accès aux données de la Banque-carrefour des Entreprises[80].

Le *Comité sectoriel de la sécurité sociale et de la santé* est divisé en deux sections : la section « sécurité sociale » et la section « santé ». La section « sécurité sociale » est compétente, en somme, pour contrôler les traitements de données effectués par les institutions de sécurité sociale[81].

Par ailleurs, la section « santé » veille à la légalité des traitements de données à caractère personnel relatives à la santé, au sens de la loi du 8 décembre 1992[82].

Le *comité de surveillance sectoriel « Phénix »* contrôle les traitements des données issues de la banque de données Phénix[83], qui est la banque de données de l'ordre judiciaire.

Le *comité de surveillance statistique* est compétent pour autoriser la Direction générale statistique du SPF Économie à communiquer des données d'étude codées[84].

Enfin, le *comité sectoriel pour l'Autorité fédérale* a une compétence résiduelle, en ce qu'il est compétent pour autoriser « toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, (…) à moins que la communication n'ait déjà fait l'objet d'une autorisation de principe d'un autre comité sectoriel créé au sein de la Commission pour la protection de la vie privée »[85].

15. Les autorisations dans le réseau fédéral

Avant de s'adresser à Fedict, l'administration demanderesse de données à caractère personnel doit obtenir, de la part du comité sectoriel compétent, l'autorisation d'accéder à ces données. Fedict vérifiera que cette autorisation a été octroyée avant de procéder à l'acheminement des données réclamées[86]. Ainsi, par exemple, une administration qui a besoin des coordonnées d'un citoyen devra obtenir l'autorisation du Comité sectoriel du Registre national pour accéder à ces données.

De plus, la loi du 15 août 2012 prévoit qu'au sein du réseau fédéral, les citoyens sont identifiés à partir de leur numéro d'identification au Registre national[87]. Dès lors, lorsqu'une administration s'adresse à Fedict, elle lui indique le numéro d'identification de la personne dont elle souhaite obtenir les données, plutôt que ses nom et prénom, par exemple. Le numéro d'identification au Registre national étant propre à chaque personne, son utilisation permet de ne pas confondre les citoyens entre eux. Néanmoins, ce numéro d'identification est une donnée à caractère personnel dont l'utilisation n'est pas libre. L'administration concernée doit demander au Comité sectoriel du

[77] Le pouvoir de décision des comités sectoriels institués au sein de la Commission de la protection de la vie privée soulève la question de savoir si les décisions rendues sont attaquables devant le Conseil d'État. Cette question est complexe et dépasse l'objet de la présente étude. Nous nous permettons de renvoyer le lecteur aux développements repris dans l'ouvrage suivant : E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os^ 576 et s.

[78] Article 5 de loi du 8 août 1983 sur le Registre national. Voy. également l'article 15 de cette même loi.

[79] *Ibidem,* articles 8 et 15.

[80] Articles 17 et 18, § 2, du 16 janvier 2003 portant création d'une Banque-carrefour des Entreprises, *M.B.*, 5 février 2003.

[81] Ce terme doit être compris au sens de l'article 2, 2°, de la loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale. Voy. égal. l'article 43*bis*, alinéa 1, de cette loi.

[82] Article 43*bis,* alinéa 2, de la loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale. Voy. également l'article 42, § 2, 3°, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, *M.B.*, 22 décembre 2006. Ainsi, sont soumis à l'autorisation de la section « sécurité sociale » et non à celle de la section « santé », les traitements de données à caractère personnel relatives à la santé, au sens de la loi du 8 décembre 1992, par les institutions de sécurité sociales et les personnes visées à l'article 18 de la loi du 15 janvier 1990 (article 15, § 2, 2°, et article 43*bis* de la loi du 15 janvier 1990) ; les traitements de données sociales à caractère personnel relatives à la santé (au sens de la loi du 15 janvier 1990) par les instances d'octroi visées à l'article 11*bis* de la loi du 15 janvier 1990 (article 43*bis* de la loi du 15 janvier 1990) et les traitement de données sociales à caractère personnel relatives à la santé par une instance de sécurité sociale vers une autre instance de sécurité sociale, une instance d'octroi visée à l'article 11*bis* de la loi du 15 janvier 1990 ou une personne visée à l'article 18 de la loi du 15 janvier 1990 (article 15, § 1, de la loi du 15 janvier 1990). Sur la question de la compétence d'autorisation de chaque section de ce comité sectoriel, voy. également CPVP, avis n° 43/2006 du 8 novembre 2006 relatif au projet de loi portant dispositions diverses – création d'un comité sectoriel de la sécurité sociale et de la santé, p. 7, n° 15.

[83] Articles 22 et s. de la loi du 10 août 2005 instituant le système d'information Phénix, *M.B.*, 1^er^ septembre 2005.

[84] Article 17 de la loi du 22 mars 2006 modifiant la loi du 4 juillet 1962 relative à la statistique publique et la loi du 8 août 1983 sur le Registre national. Voy. également l'article 35 de cette même loi ainsi que l'arrêté royal du 7 juin 2007 fixant les modalités relatives à la composition.

Les données d'étude sont « les informations qui serviront à établir des résultats statistiques ». On les dit « codées » lorsqu'elle « ne peuvent être mises en relation avec une personne identifiée que par l'intermédiaire d'un code » [article 3 de la loi du 22 mars 2006 modifiant la loi du 4 juillet 1962 relative à la statistique publique et la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.*, 21 avril 2006. Signalons que cette disposition n'est pas encore entrée en vigueur].

[85] Article 36*bis* de la loi du 8 décembre 1992.

[86] Article 8, § 2, de la loi du 15 août 2012.

[87] Article 5, § 1, de la loi du 15 août 2012. Précisons néanmoins que pour les personnes physiques qui ne sont pas enregistrées au Registre national et pour toute autre information (telles que les données relatives aux entreprises), Fedict devra, à l'avenir, développer d'autres numéros d'identification (à ce sujet, voy. les discussions préparatoires à l'adoption de la loi du 15 août 2012, Exposé des motifs, *Doc. parl.*, Ch. Repr., session 2011-2012, n° 53-2223/001, pp. 23 et 24).

Registre national l'autorisation de pouvoir l'utiliser[88].

En somme, chaque administration du réseau fédéral doit donc demander au Comité sectoriel du Registre national l'autorisation d'utiliser, dans ses échanges avec Fedict, le numéro d'identification des personnes physiques enregistrées au Registre national. Ensuite, chaque administration doit également demander une autorisation pour toutes les données auxquelles elle souhaite accéder via Fedict. Cette demande doit être adressée au comité sectoriel compétent, déterminé en fonction du type de données concerné.

Signalons qu'une demande d'autorisation prend la forme d'un dossier complet établissant le respect d'un certain nombre de conditions[89]. En pratique, cette tâche peut s'avérer fastidieuse. C'est pourquoi, certains intégrateurs de services proposent une aide précieuse aux administrations concernées. Par exemple, la Banque-carrefour d'échanges des données, qui est l'intégrateur de services horizontal de la Région wallonne et de la Communauté française, propose aux administrations qui doivent collecter indirectement des données par son intermédiaire de les aider à rédiger les demandes d'autorisation qui seront soumises aux comités sectoriels compétents[90]. Cette méthode encourage les administrations à rédiger une demande de qualité et facilite, dans le même temps, le travail des comités sectoriels saisis des demandes. Il serait judicieux que Fedict s'inspire de cette pratique pour faciliter la tâche des administrations fédérales.

C. Répondre à l'exercice des droits d'accès et de rectification du citoyen

16. Les risques d'erreur et d'abus dans l'utilisation des données

La collecte unique des données facilite la tâche des administrations et des citoyens mais risque de provoquer un sérieux dysfonctionnement administratif si les sources authentiques de données contiennent des données incorrectes. En effet, la mise en œuvre de la collecte unique des données est fondée sur une réutilisation maximale des données issues des sources authentiques. Si une donnée est erronée, un « effet domino »[91] se produit puisque l'erreur est démultipliée autant de fois que la donnée est réutilisée. Le travail de l'ensemble des administrations ayant utilisé la donnée échangée en pâtit alors. Il pourrait donc arriver qu'un citoyen soit soumis à une décision administrative fondée sur une donnée erronée. Dans cette hypothèse, on peut raisonnablement penser que, étonné face à pareille décision, il veuille comprendre d'où vient l'erreur. Contactant l'administration ayant pris cette décision, celle-ci pourrait lui répondre que les informations sur la base desquelles a été prise ladite décision administrative lui ont été fournies par l'intégrateur de services et qu'elle n'en connaît pas l'origine. Face à pareille situation, comment le citoyen peut-il savoir où se trouve ses données et obtenir que les erreurs les affectant éventuellement soient corrigées ?

Par ailleurs, chaque citoyen est contraint de donner à l'administration un grand nombre d'informations relatives à de nombreux aspects de leur vie personnelle : coordonnées, composition de ménage, numéro de téléphone, situation financière, caractéristiques médicales justifiant l'octroi d'une allocation pour personne handicapée, etc. Ces informations étant aujourd'hui enregistrées électroniquement dans des bases de données, elles sont aisément et rapidement accessibles. Il peut donc être tentant, pour un agent de l'administration, de céder à la curiosité et d'aller consulter des informations auxquelles il a accès depuis son ordinateur. On pense, par exemple, à la consultation du registre DIV par des policiers ayant repéré, sur la route, de jolies conductrices à qui ils désirent téléphoner, ou encore à la consultation du Registre national par un fonctionnaire communal dans le but de retrouver l'adresse de son ancienne compagne[92]. Il s'agit là d'utilisations abusives des bases de données de l'administration, qui doivent être sanctionnées. Encore faut-il pouvoir établir qui a accédé illégalement à quelles informations.

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

[88] Article 8 de la loi du 8 août 1983 relative au Registre national. Précisons que Fedict n'est pas soumis à cette obligation. Pour lui éviter de devoir demander l'autorisation du Comité sectoriel du Registre national pour chaque transfert de données qu'il effectue, l'article 5, § 1, de la loi du 15 août 2012 lui confère une autorisation générale d'utiliser le numéro d'identification au Registre national.

[89] Un questionnaire détaillé doit être rempli, qui varie selon le comité sectoriel compétent. Ces questionnaires se trouvent sur le site de la Commission de la protection de la vie privée. Voy. par exemple, le questionnaire d'accès à des données du Registre national repris à l'adresse http://www.privacycommission.be/sites/privacycommission/files/documents/formulaire-demande-autorisation-rn.pdf.

[90] À ce sujet, voy. la fiche méthodologique que la Banque-carrefour d'échanges de données propose aux administrations de la Région wallonne et de la Communauté française, disponible à l'adresse http://www.ensemblesimplifions.be/sites/default/files/sites/all/files/10300.eWBS-FM.partage_de_donne %CC %81es_et_BCED.pdf.

[91] CPVP, avis n° 11/2009 du 29 avril 2009 concernant le projet d'arrêté du Gouvernement flamand portant exécution du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, p. 3, n° 6.

[92] À ce sujet, voy. not., C.E., *Van Merris,* arrêt n° 143.683 du 26 avril 2005.

17. Le droit d'accès et de rectification

Chaque citoyen a le droit de connaître un bon nombre d'informations relatives à l'usage qui est fait de ses données[93]. Il peut donc s'adresser à chaque administration qui détient des données à son sujet en demandant les données exactes qui figurent dans son dossier, les raisons pour lesquelles elle sont enregistrées, à qui elles ont déjà été transmises et/ou le seront ultérieurement, pendant combien de temps seront-elles conservées, etc[94]. S'il constate des erreurs dans ces données, il a le droit d'exiger qu'elles soient rectifiées. Néanmoins, la procédure actuelle d'accès et de rectification des données est fastidieuse. Il faut envoyer à chaque administration une lettre signée et accompagnée d'une photocopie de la carte d'identité, en indiquant clairement les informations que l'on recherche. L'administration dispose de 45 jours pour répondre à la demande, et éprouve souvent elle-même des difficultés pour réaliser ce travail. En outre, l'exercice de ces droits est particulièrement fastidieux dans le contexte de l'administration en réseaux puisque l'enregistrement des données est éparpillé entre diverses sources authentiques du réseau si bien qu'il est difficile de deviner quelle institution détient quelle donnée.

La loi du 15 août 2012 organise des solutions qui pourraient être de nature à alléger les démarches du citoyen, pour autant qu'elles soient adéquatement développées à l'avenir. Ainsi, s'agissant de la rectification des données erronées circulant au sein du réseau fédéral, l'article 16, § 1, de la loi du 15 août 2012 affirme qu'il revient à l'intégrateur de services et aux services publics participants de déterminer « des canaux d'accès » afin que le citoyen puisse introduire ses requêtes d'adaptation des données. En outre, pour répondre au souci d'identifier notamment les abus dans l'utilisation des données, l'article 14 prévoit que, pour chaque échange de données réalisé par l'intermédiaire de l'intégrateur de services fédéral, il faut qu'« une reconstruction complète puisse avoir lieu (…) de quelle personne physique a utilisé quel service relatif à quelle personne, quand et à quelles fins »[95]. Il s'agit donc de pouvoir identifier le parcours suivi par les données échangées au sein du réseau fédéral, ce que l'on appelle également un « *audit trail* »[96]. En outre, dans la lignée de cette disposition, l'article 16, § 2, de la loi du 15 août 2012 affirme que la personne concernée « a le droit de savoir quelles autorités, quels organismes ou quelles personnes ont, au cours des six mois écoulés, consulté ou mis à jour ses données par le biais du réseau ». Et de conclure en affirmant que « l'intégrateur de services fédéral prévoit les moyens techniques appropriés pour assurer l'exécution (…) de l'article 14 »[97].

En somme, il revient désormais à Fedict de développer les canaux nécessaires pour permettre à chaque personne d'obtenir la rectification de ses données et de visualiser le parcours suivi par ses données au sein du réseau fédéral.

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

18. Le portail « Mon dossier » du Registre national

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

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

[93] Article 10 de la loi du 8 décembre. Voy. égal. l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001 ; E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, ibidem,* n° 331 et s. Pour un cas d'application dans l'administration, voy. Cass. (1re ch.), 14 janvier 2013, *R.D.T.I.*, 2013, pp. 53 et s, note E. Degrave « Transparence administrative et traitements de données caractère personnel ».

[94] À cet égard, signalons que, pour faciliter la tâche du citoyen, la Commission de la protection de la vie privée a établi une lettre type comprenant notamment la liste des types d'informations qui peuvent être demandées au responsable de traitement. Il revient au demandeur d'accès de cocher dans cette liste ce qu'il souhaite se voir communiquer. Cette lettre type est disponible sur le site internet de la Commission de la protection de la vie privée à l'adresse http://www.privacycommission.be/fr/exercice-droit-acces/vos-possibilites.

[95] Article 14, alinéa 4, de la loi du 15 août 2012.

[96] À ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.,* nos 400 et s.

[97] Article 16, dernier alinéa, de la loi du 15 août 2012.

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

a) Les données de contenu

Le citoyen peut consulter les données enregistrées à son sujet dans la source authentique qu'est le Registre national, telles que ses nom, prénoms, date de naissance, adresse mais également la profession, des données relatives à son permis de conduire, à sa participation aux élections, etc. Par ailleurs, le portail mentionne clairement la possibilité pour la personne d'exercer son droit de rectification auprès de sa commune, si une erreur affecte ses données à caractère personnel[98]. L'exercice du droit de rectification est facilité par la présence d'un hyperlien contenant l'adresse mail de la commune. Enfin, une rubrique « transactions » permet au citoyen d'obtenir les documents officiels reprenant ses données tels qu'une composition de ménage, un certificat de nationalité, un extrait de registre de la population, ou de créer lui-même un document en sélectionnant les données qui doivent s'y trouver, ce qui lui permet d'éviter un déplacement à la commune lorsqu'il a besoin de produire une copie de ces documents.

b) Les données de consultation

En cliquant sur la rubrique « Historique des consultations », la personne concernée peut connaître, en principe, « toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consulté ou mis à jour ses données au registre de la population ou au registre national des personnes physiques »[99]. Comme l'a affirmé la Commission de la protection de la vie privée, cette mesure vise notamment à « permettre au citoyen de jouer un rôle d'avertisseur, puisqu'il est le mieux placé pour détecter des consultations 'anormales'pouvant donner lieu à des sanctions »[100]. Le citoyen ne voit apparaître que la désignation de l'institution qui a consulté ses données, mais non le nom de l'agent[101]. Si le citoyen constate une consultation suspecte de ses données, il peut s'adresser à l'institution désignée sur le portail internet afin de lui demander davantage de précisions sur cette consultation, telles que, par exemple, le nom de l'agent ayant effectué cette consultation et la raison pour laquelle il l'a effectuée.

C'est pourquoi, parallèlement à ce qui figure dans l'application « Mon dossier », les administrations dont les agents ont accès au Registre national doivent disposer, en interne, d'un système qui enregistre l'identité des fonctionnaires chaque fois qu'ils effectuent une consultation de la source authentique[102]. À cette fin, par exemple, certaines communes tiennent un registre dans lequel les agents notent les raisons précises pour lesquelles ils ont consulté le Registre national. Ce faisant, si un citoyen demande des éclaircissements à propos d'une consultation en particulier, l'agent concerné pourra fournir les précisions requises. Au-delà de cet aspect, un tel système permet à l'institution de contrôler ses agents, notamment si une augmentation anormale de consultations est constatée en provenance de l'un d'eux. Enfin, on peut raisonnablement penser que le fait, pour les fonctionnaires, de savoir que leur identité est enregistrée et qu'il existe dès lors une possibilité de contrôler leurs agissements en ce domaine soit de nature à les inciter à faire bon usage du Registre national.

V. LES SANCTIONS MENAÇANT LES ADMINISTRATIONS ET LEURS AGENTS

19. Les sanctions applicables aux agents de l'administration

Si un agent[103] méconnaît l'une des obligations organisées par la loi du 15 août 2012, il risque de se voir infliger une sanction pénale[104]. Ainsi, par exemple, un agent qui consulte, à des fins person-

[98] La procédure est réglée par l'annexe 1er de la circulaire du 23 juin 2008 relative à l'application de l'arrêté royal du 19 mars 2008 organisant la procédure de communication des différences constatées entre les informations du Registre national des personnes physiques et celles des registres visés à l'article 2 de la loi du 8 août 1983 organisant un Registre national des personnes physiques, publié au *Moniteur belge* du 15 avril 2008.

[99] Article 6, § 3, 3°, de la loi du 19 juillet 1991 précitée. Voy. égal. l'arrêté royal du 13 février 2005 déterminant la date d'entrée en vigueur et le régime du droit de prendre connaissance des autorités, organismes et personnes qui ont consulté ou mis à jour les informations reprises dans les registres de population ou au registre national des personnes physiques, *M.B.*, 28 février 2005.

[100] CPVP, avis n° 12/2009 du 29 avril 2009 relatif à une demande d'avis émanant du SPF Intérieur concernant un certain nombre de questions qui se sont posées dans la délibération RN n° 19/2008, p. 6.

[101] Il s'agit là d'une mesure de protection de la vie privée des agents de l'administration. A ce sujet, voy. CPVP, avis n° 12/2009 du 29 avril 2009 relatif à une demande d'avis émanant du SPF Intérieur concernant un certain nombre de questions qui se sont posées dans la délibération RN n° 19/2008, p. 6.

[102] À ce sujet, voy. CPVP, avis n° 12/2009 précité, p. 8.

[103] Les travaux préparatoires de la loi du 15 août 2012 mentionnent que ces sanctions pénales s'appliquent « tant au personnel de l'intégrateur de services fédéral, du service public et de l'ASBL Egov actif au sein du service public qu'aux consultants externes de sous-traitants qui exécutent un marché pour le service public, etc. » (voy. Projet de loi relatif à la création et à l'organisation d'un intégrateur de services fédéral, *op. cit.*, n° 53- 2223/001, p. 37).

[104] Voy. les articles 37 et s. de la loi du 15 août 2012. Remarquons que les sanctions pénales prévues par la loi du 15 août 2012 ne visent pas toutes les hypothèses d'abus dans l'utilisation des données. Pour celles qui ne sont pas mentionnées dans cette loi, il y a lieu de se référer aux articles 550*bis* et 550*ter* du Code pénal, ainsi qu'aux dispositions pénales organisées par la loi du 8 décembre 1992 (articles 36*ter* et s.).

nelles, les données du Registre national d'un tiers, risque une peine d'emprisonnement de huit jours à six mois et une amende de cent euros à cinq mille euros[105]. Plusieurs facteurs peuvent expliquer la gravité de la peine attribuée *in fine* à l'agent tels que l'utilisation des données à des fins privées ou pour des tiers, le fait que l'agent commet une illégalité pour la première fois ou non, sa qualité au sein du service[106], etc.

Ces sanctions individuelles soulignent donc à nouveau l'importance, pour l'administration, de mettre en place un système permettant d'identifier les agents ayant consulté une base de données, comme nous le soulignions plus haut[107].

Par ailleurs, les sanctions pénales organisées par la loi du 15 août 2012 sont sévères, afin de dissuader toute personne d'abuser des données circulant au sein du réseau fédéral. En effet, comme l'affirme le législateur, cette loi « traite une matière sensible qui concernera souvent la vie privée des intéressés. Les conséquences éventuelles d'un abus du réseau peuvent donc aussi être considérables et nécessitent dès lors des dispositions pénales efficaces »[108].

Néanmoins, au-delà de cet objectif de dissuasion et de punition, le bon fonctionnement de l'administration en réseau gagnerait à ce que les agents aient une bonne connaissance de ces règles et de leur importance. Ainsi, il serait judicieux d'amener les agents de l'administration à suivre une formation en matière d'e-gouvernement, qui insisterait notamment sur les règles qu'ils doivent respecter et la manière de les mettre en œuvre adéquatement. Cette formation pourrait être proposée à tous les agents de l'administration et imposée à ceux qui ont commis des abus dans l'usage des données qu'ils traitent.

20. Les sanctions applicables aux décisions de l'administration

Indépendamment des sanctions pénales applicables aux agents de l'administration, il ne faut pas perdre de vue que les décisions administratives illégales peuvent elles-mêmes être frappées de sanction. En effet, ainsi qu'on l'a déjà dit, la loi du 15 août 2012 et la loi du 8 décembre 1992 imposent aux administrations de nouvelles obligations, y compris au stade des mesures préparatoires des actes administratifs. Un acte administratif pris en violation de ces obligations risquerait d'être annulé par le Conseil d'État.

Plus particulièrement, une décision administrative fondée sur un traitement de données à caractère personnel doit respecter certaines *conditions de fond* imposées par la loi du 15 août 2012 et la loi du 8 décembre 1992. Par exemple, comme dit précédemment, l'administration est soumise à l'obligation de collecte indirecte des données qui sont disponibles dans le réseau. Dès lors, si l'administration refuse l'octroi d'un avantage au citoyen au motif qu'il n'a pas fourni le renseignement requis alors que celui-ci était disponible dans le réseau, cette décision est illégale et pourrait être censurée par un juge.

Les administrations sont également tenues au respect de *formalités* propres au régime de la protection des données à caractère personnel. On pense notamment à l'obligation pour une administration d'obtenir l'autorisation du comité sectoriel compétent en cas de collecte indirecte de données[109]. Ces formalités doivent obligatoirement être respectées. Un acte administratif qui les méconnaîtrait serait illégal et, partant, pourrait être annulé par le Conseil d'État.

Par ailleurs, un juge judiciaire pourrait également être amené à ne pas appliquer une décision administrative fondée sur un traitement de données illégal, en vertu de l'article 159 de la Constitution. Par exemple, si une administration utilise des données du Registre national qu'elle détient dans une base de données interne, sans demander au préalable à Fedict la mise à jour de ces données afin de s'assurer de leur exactitude, elle risque d'adopter une décision fondée sur des données fausses. Dans cette hypothèse, la décision administrative viole l'obligation d'utiliser des données de qualité[110] et doit être écartée par le juge judiciaire.

CONCLUSIONS

L'administration doit à présent s'engager pleinement dans l'e-gouvernement et la simplification administrative, tant pour alléger les tâches des citoyens que pour améliorer sa propre efficacité. Loin de n'être qu'un apprivoisement des nouveaux outils informatiques, le passage de l'administration en silos à l'administration en réseaux est un bouleversement dans la structure et le fonctionnement de l'administration. La réussite de ce défi suppose donc de nombreux changements d'habitude au sein des institutions publiques.

[105] Voy. article 37 de la loi du 15 août 2012.

[106] Projet de loi relatif à la création et à l'organisation d'un intégrateur de services fédéral, *op. cit.*, n° 53- 2223/001, p. 38.

[107] Voy. *supra*, IV, C, n° 17.

[108] Projet de loi relatif à la création et à l'organisation d'un intégrateur de services fédéral, *op. cit.*, n° 53- 2223/001, pp. 36 et 37.

[109] Article 8, § 2, de la loi du 15 août 2012.

[110] Article 4, 4°, de la loi du 8 décembre 1992, auquel renvoie l'article 5, § 2, de la loi du 15 août 2012.

Ainsi, puisque, depuis l'entrée en vigueur d'une loi du 5 mai 2014, les agents de l'administration fédérale sont désormais obligés d'utiliser l'intégrateur de services fédéral en s'adressant au SPF Fedict, ils doivent renoncer à attendre du citoyen qu'il communique lui-même les informations déjà disponibles dans le réseau fédéral et les trouver par eux-mêmes. Cette obligation de collecte indirecte génère une multiplication des traitements de données à caractère personnel des citoyens, ce qui explique également que de nouvelles mesures doivent être mises en place au sein de chaque institution du réseau fédéral, notamment pour respecter le régime juridique de la protection de la vie privée et des données à caractère personnel. Un conseiller en sécurité doit être engagé et les agents doivent être formés pour répondre aux droits d'accès et de rectification des citoyens. De plus, avant de s'adresser au SPF Fedict, chaque institution concernée doit introduire une demande d'autorisation auprès du comité sectoriel compétent pour autoriser l'utilisation des données recherchées dans le réseau.

Il faut saluer le fait que la collecte indirecte des données soit aujourd'hui une obligation légale assortie de sanctions et non une simple bonne pratique administrative. Les administrations et leurs agents seront incités à utiliser l'intégrateur de services et à respecter ces contraintes nouvelles, ce qui permettra de concrétiser et de généraliser davantage la simplification administrative. Au-delà des économies de temps et d'argent qui en résulteront, l'obligation de collecte indirecte favorisera aussi le respect du principe de la réciprocité des avantages qui veut que le citoyen bénéficie des avantages que la technologie offre à l'administration, en étant lui-même allégé dans ses charges administratives.

Néanmoins, la collecte indirecte des données doit être accompagnée de mesures corollaires à l'égard desquelles le SPF Fedict semble, pour l'heure, accuser un certain retard. Pour cette raison, les administrations risquent d'éprouver prochainement des difficultés à respecter l'obligation de collecte indirecte tandis que les citoyens pourraient ne pas comprendre clairement l'impact de cette obligation nouvelle sur les dossiers qui les concernent. On a ainsi pointé le manque de transparence qui entoure l'intégrateur de services fédéral et le réseau fédéral. Pour remédier à cette lacune, il devient urgent de développer la visibilité des sources authentiques de données et des types de données disponibles dans le réseau fédéral, de manière à ce que les administrations et les citoyens identifient les informations soumises à l'obligation de collecte indirecte. Il est également impératif que le citoyen puisse exercer son droit d'accès aux données à caractère personnel et son droit de rectification de celles-ci plus aisément qu'actuellement. Le Registre national offre, à cet égard, un outil intéressant que le SPF Fedict pourrait reprendre pour le réseau fédéral. Par ailleurs, les données actuellement accessibles via le SPF Fedict sont relativement peu importantes puisqu'il s'agit uniquement des informations du Registre national, du Registre *bis* et de celles de la Banque-carrefour des entreprises. La simplification administrative gagnerait à ce que le réseau fédéral compte d'autres sources authentiques de données et que le SPF Fedict organise de nouveaux flux de données au sein de ce réseau. Parallèlement à cela, compte tenu de la complexité de la matière en cause, les administrations devraient pouvoir être aidées dans la rédaction des demandes d'autorisation au comité sectoriel compétent. S'agissant de ces aspects, la Banque-carrefour d'échanges des données, qui œuvre au niveau de la Région wallonne et de la Communauté française, a déjà réalisé d'intéressantes avancées qui pourraient constituer une source d'inspiration utile pour le réseau fédéral.