UCLouvain

Faculté de droit et de criminologie

LA CIRCULATION DES DONNÉES DE SANTÉ

Analyse de la légitimité des plateformes d'échange des données de santé au regard de la protection des données personnelles par le droit européen

Auteur : François HARDY

Promoteur : Alain STROWEL

Année académique 2020-2021

DROI2MS/EU - Master [120] en droit, à finalité spécialisée : Droit européen

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

REMERCIEMENTS

Je souhaite adresser quelques « mercis » à certaines personnes en particulier :

Un merci respectueux à mon promoteur de mémoire, M. Alain Strowel, pour ses réorientations pragmatiques et pour sa réactivité, même dans les dernières semaines ;

Un merci reconnaissant à mes deux parents : à mon papa pour les conditions de travail optimales dont j'ai toujours pu bénéficier ; à ma maman, pour sa relecture minutieuse de ce mémoire ;

Un merci chaleureux à mes deux colocataires : à Emma, l'optimisme incarné, pour y avoir toujours cru ; à Tanguy, le réalisme incarné, pour m'avoir maintenu une pression bienvenue ;

Un merci loyal à mon amie Zoé, pour m'avoir suivi pendant tout le Master, et pour m'avoir permis de relativiser en constatant qu'il y a toujours pire galère que la mienne ;

Enfin, un merci tout particulier à mon grand-père, qui m'aura indiscutablement insufflé tout le courage nécessaire, de là où il s'en est allé, exactement au moment où j'en ai eu besoin.

« *Les données et l'intelligence artificielle sont les ingrédients de l'innovation qui peuvent nous aider à trouver des solutions aux enjeux sociétaux actuels dans le domaine de la santé.*

Afin de réaliser tout ce potentiel, nous devons trouver notre propre voie européenne, en équilibrant le flux et la large utilisation des données, tout en préservant un haut degré de protection de la vie privée, de sécurité, de sûreté et d'éthique.

Je crois que l'Europe peut réussir ce passage à l'ère numérique, si elle s'appuie sur ses forces et ses valeurs. »[1]

URSULA VON DER LEYEN,

[1] U. VON DER LEYEN, *Une Union plus ambitieuse. Mon programme pour l'Europe - Orientations politiques pour la prochaine Commission européenne 2019-2024*, 16 juillet 2019, pp. 15-16.

Table des matières

Introduction

La quantité de données échangées dans le monde à l'heure actuelle est devenue impossible à chiffrer précisément. Les dernières études menées à grande échelle avaient estimé en 2018 que « *tous les deux jours, l'humanité produit autant d'informations que ce qu'elle a généré durant la période antérieure à 2003, ce qui représente chaque année près d'un zettaoctet* [(ce qui équivaut à 1.000.000.000.000.000.000.000 d'octets)] *d'informations numériques* »[2]. Les quantités réelles sont même probablement encore bien au-dessus de ces estimations. La haute valeur de ces données a rapidement révélé leur immense potentiel, tous secteurs confondus.

Un de ces secteurs a été mis particulièrement en avant dans le contexte sanitaire que l'on connait actuellement. Les confinements successifs ont accentué la télémédecine, les stratégies de *testing*, dans un premier temps, et de vaccination, dans un second temps, ont nécessité de nouvelles applications en ligne, et la charge toujours plus lourde sur les hôpitaux a renforcé le besoin d'une gestion efficace des soins de santé en Belgique et dans l'Union européenne.

Même avant la crise sanitaire, la rencontre de ces deux thématiques a inévitablement fait remonter dans l'agenda politique la nécessité d'instaurer une bonne circulation des données relatives à la santé des patients. L'échange de données médicales est en effet une étape essentielle dans le développement numérique d'un gouvernement démocratique. Mais à tout moment, le citoyen avisé se posera la question de la sécurité de ses données de santé : « Où sont les données relatives à ma santé ? », « Qui peut consulter ma prise de médicaments et mes antécédents de maladie ? », et fatalement « Comment puis-je être certain que toutes ces informations sont en sécurité là où elles sont ? ». Conscient de l'attachement du citoyen à la protection de sa vie privée et de ses données personnelles, l'autorité publique a mis en place, on le verra, différentes plateformes d'échange des données de santé, mais également toutes sortes d'instruments destinés à garantir au citoyen ses droits les plus fondamentaux.

[2] R. TINIÈRE, « L'apport de la Charte des droits fondamentaux à la protection des données personnelles dans l'Union européenne », *Rev. Aff. Eur.*, 2018, p. 29.

Présentation de la question de recherche

La présente analyse a pour objet principal de tester la légitimité de ces différentes plateformes, par lesquelles transitent tous les jours les données de santé du citoyen belge. À cet égard, elle tentera de vérifier la compatibilité entre, d'une part, les dispositions légales concernées, et, d'autre part, le fonctionnement concret de trois plateformes d'échange des données de santé.

On commencera donc par déterminer le cadre légal pertinent en la matière (Partie I). Ce sera l'occasion d'exposer toutes les règles qui entourent, d'une part, la protection des données de santé actuellement, et, d'autre part, celles qui circonscrivent l'échange de celles-ci. Au travers d'une approche plus pratique, on expliquera ensuite le fonctionnement précis de trois plateformes qui permettent, ou permettront, une circulation fluide et efficace des données de santé, tant au niveau belge qu'au niveau européen (Partie II). La dernière partie de cette analyse sera consacrée à une réflexion critique, qui exploitera réellement cette question de la légitimité des plateformes précédemment expliquées, en confrontant les parties I et II pour en tirer les conclusions qui s'imposent (Partie III).

Partie I. Cadre légal

Notre analyse du cadre légal actuellement pertinent se penchera tour à tour sur les deux aspects, sur les deux enjeux qui sous-tendent la question de recherche. On verra donc dans un premier temps comment le droit belge, européen et international s'attèle à protéger les données relatives à notre santé (Titre I). Dans un second temps, l'analyse légale se tournera vers le cadre qui existe actuellement autour de l'échange des données, personnelles ou non (Titre II).

Titre I. Protection des données médicales

Tant au niveau national qu'au niveau européen, les données relatives à notre santé bénéficient d'un niveau de protection élevé. Il convient de procéder selon une démarche en escalier, de façon à atteindre progressivement ce niveau élevé de protection. Sauter une marche risquerait de mettre en péril une telle progression. C'est pourquoi, après avoir dressé un tableau des enjeux soulevés par la question (chapitre I), on verra d'abord la protection générale de la vie privée (chapitre II), puis la protection plus spécifique des données personnelles (chapitre III), pour enfin parvenir à la protection renforcée de certaines catégories particulières de données personnelles (chapitre IV).

Chapitre I. Enjeux de la protection des données médicales

Dans la sphère de la santé, les enjeux concernant la protection des données relatives à la santé du patient sautent aux sont évidents, tant la santé touche au cœur de notre vie privée. Si cette analyse aura tendance à aller dans le sens d'une maximisation des échanges de données, il ne faudrait pas non plus tomber dans des excès, sans garder aucune considération de la vie privée du patient.

Par exemple, il ne faudrait pas que les plateformes d'échange des dossier médicaux globaux des patients, une fois mises en place, permettent à n'importe quel médecin d'accéder aux données de n'importe quel patient, sans qu'il existe entre eux de lien de soins médicaux. Cela s'applique tant à la sphère familiale (une personne qui aurait un oncle médecin ne souhaite

pas forcément que celui-ci soit au courant de ses antécédents de santé) qu'à la sphère professionnelle (il ne faudrait pas qu'un futur employeur, simplement parce qu'il connait un médecin dans son entourage proche, puisse accéder, via ce dernier, à la prise de médicaments de son potentiel futur employé).

Dans le même ordre d'idées, si l'on pousse la réflexion un cran plus loin que les strictes données relatives à la santé, il serait dangereux de fournir un accès trop large à nos données génétiques. L'exemple peut paraître saugrenu, mais il est aujourd'hui tout à fait possible de partager, sur les réseaux sociaux, toute sortes d'informations sur notre santé, obtenues à des prix dérisoires auprès de différentes biotechs[3] américaines. Typiquement, un assureur-vie aurait grand intérêt à connaître les prédispositions génétiques à certaines maladies graves de ses potentiels contractants. Mais à nouveau, cela dépasse le cadre de cette analyse.

Chapitre II. Vie privée

Pour cette première étape, il est nécessaire de tout d'abord essayer de définir le concept de « vie privée ». Comme on le verra, il s'agit d'une tâche difficile car la définition ne vient pas d'elle-même (Section 1). Cela fait, on pourra tour à tour examiner comment ce droit à la vie privée est protégé par les différents instruments légaux qui nous concernent (Section 2). On terminera le chapitre en expliquant le lien qui existe entre la vie privée et les données personnelles, lien qui nous permettra de passer à la seconde marche de l'escalier (Section 3).

Section 1. Définition

Le concept de « vie privée » est une notion vaste. Si vaste qu'il est difficile de la définir de manière exhaustive[4]. La Cour européenne des droits de l'homme ne juge d'ailleurs « *ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de* 'vie privée'. »[5].

[3] On peut mentionner, à titre d'exemple, la biotech américaine *23andMe*, qui proposait, pour une somme raisonnable, d'envoyer au client une analyse détaillée de sa généalogie et de ses prédispositions à certaines maladies, sur base d'une analyse génétique d'un échantillon de salive qu'il lui envoyait par courrier ; https://www.23andme.com/, consulté le 12 février 2021.

[4] *Guide sur l'article 8 de la Convention européenne des droits de l'homme*, Conseil de l'Europe, 31 août 2020.

[5] Cour eur. D.H., arrêt *Niemitz c. Allemagne*, 16 décembre 1992, §29.

La haute juridiction se limite, lorsqu'elle doit déterminer si l'affaire en cause relève du champ d'application de la vie privée, à citer différents éléments qui entrent dans sa sphère personnelle[6].

Le professeur Yves Poullet, professeur émérite de l'Université de Namur et ancien recteur, s'est toutefois essayé à une définition du droit à la vie privée. Selon ses mots, « *la notion unifie l'ensemble des prérogatives qui apparaissent nécessaires pour amener le développement de la personnalité de l'individu dans une société donnée et pour assurer ainsi la vitalité de nos sociétés démocratiques* »[7].

S'il reste difficile de bien délimiter le champ du concept de vie privée, on peut toutefois tenter de caractériser la notion. Le concept de droit à la vie privée affiche une double dimension. Sa dimension horizontale vise la relation qu'un individu entretient avec un autre. Sous cette dimension, tout individu a le droit de garder un certain niveau de vie privée par rapport aux autres. La dimension verticale du droit à la vie privée recouvre la relation qui existe entre l'individu et l'autorité publique. À travers elle, le citoyen peut exercer des prérogatives vis-à-vis de l'État afin de se garantir le même niveau de vie privée[8]. Concernant la dimension verticale du droit à la vie privée, on peut pousser l'analyse un pas plus loin et affirmer que ce droit est également constitué d'une double nature. Le droit à la vie privée peut être figuré, d'une part, comme un « *droit-bouclier* », une assurance dont dispose l'individu, selon laquelle les autorités publiques s'abstiennent de toute intrusion dans sa vie privée, et, d'autre part, comme un « *droit-épée* », la revendication selon laquelle le citoyen peut exiger une série d'obligations positives aux autorités publiques, pour garantir son droit à la vie privée[9].

---

[6] Voy. par exemple Cour eur. D.H., arrêt *Pretty c. Royaume-Uni*, 29 avril 2002, §61 ; ou Cour eur. D.H., arrêt *Peck c. Royaume-Uni*, 28 janvier 2003, §57.

[7] Y. POULLET, « Le numérique et le droit à la rencontre des personnes âgées », *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, M.-C. Piatti et M. Guillermin (dir.), Paris, Editions des archives contemporaines, 2020, p. 88.

[8] S. HOEBEKE, B. MOUFFE, *Droit de la presse. Presse écrite, presse audiovisuelle et presse électronique,* Limal, Anthemis, 2012, p. 474, note de bas de page 1039 : « *Bien que l'obligation de respecter la présomption d'innocence ne s'applique pas en tant que telle à la presse, Monsieur R. est fondé à soutenir que la violation de ce principe à la suite d'un comportement fautif de la presse entraîne, le cas échéant, l'obligation pour elle de réparer le préjudice subi. Dans ce sens, l'article 8 de la Convention européenne des droits de l'homme qui protège le droit au respect de la vie privée et familiale, est d'application verticale et horizontale* ».

[9] H. DUMONT, I. HACHEZ, « Les obligations positives déduites du droit international des droits de l'Homme : dans quelles limites ? », *Les droits de l'Homme, bouclier ou épée du droit pénal ?*¸ Y. Cartuyvels, H. Dumont, F. Ost, M. Van De Kerckhove et S. Van Drooghenbroeck (dir.), Bruxelles, Bruylant, 2007, p. 63.

Section 2. Protection de la vie privée

La Constitution belge protégeait déjà certains aspects de la vie privée depuis sa rédaction en 1830. En effet, l'article 15 offrait une protection du domicile tandis que l'article 29 de la Constitution établissait le secret des lettres. En 1994 a eu lieu l'introduction de l'actuel article 22 de la Constitution, qui concerne spécifiquement la protection du droit à la vie privée. C'est donc bien après la rédaction du texte que le législateur constitutionnel a élevé la protection de la vie privée au rang suprême interne. La disposition aurait été insérée en tant que contrepartie à la publicité de l'administration (article 32 de la Constitution), qui avait été réglée simultanément[10]. On reviendra plus tard sur ce mécanisme, qui entre également en jeu dans le phénomène du partage des données. On retrouve, dans la formulation de l'article 22, la double nature du droit à la vie privée, explicitée dans la section précédente : l'alinéa 1er, d'application immédiate, transcrit l'aspect « droit-bouclier » avec les obligations négatives de l'autorité publique, tandis que l'alinéa 2 prévoit des obligations positives à charge de celle-ci : adopter des lois qui exécutent la protection de la vie privée[11]. Le droit à la vie privée, même si dorénavant élevé au rang constitutionnel, n'est pas absolu. Des restrictions à ce droit sont possibles, à certaines conditions. Même si l'article 22 de la Constitution ne mentionne que la condition de légalité, en raison de l'effet direct de la CEDH en droit belge, c'est l'ensemble des trois critères de la CEDH qui s'applique (légalité, légitimité, nécessité)[12]. Cette conclusion a été confirmée par la Cour constitutionnelle aux points B.5.5 et B.5.6 de son arrêt 151/2006 du 18 octobre 2006[13].

Si l'on a démarré le voyage de l'analyse de la protection du droit à la vie privée à Bruxelles, avec la Constitution belge, on voit toutefois rapidement que toutes les routes de cette analyse nous mènent, non pas à Rome, mais à Strasbourg. En effet, l'article 8 de la CEDH[14] protège le droit de tout individu au respect de sa vie privée et familiale. Comme déjà annoncé *supra,* la Cour européenne des droits de l'homme renonce à définir la notion de vie privée, ce qui est confirmé dans d'autres arrêts qui ont suivi[15]. À la place, elle donne une liste non

[10] K. LEMMENS, « Le droit au respect de la vie privée et de la personnalité », *Les droits constitutionnels en Belgique*, M. Verdussen et N. Bonbled (dir.), Bruxelles, Bruylant, 2011, p. 911.
[11] K. LEMMENS, *ibidem*, p. 912.
[12] K. LEMMENS, *ibidem*, p. 913
[13] C.C., 18 octobre 2006, n°151/2006, B.5.5 et B.5.6.
[14] Art. 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, *err.* 29 juin 1961.
[15] Voy. par exemple Cour eur. D.H., arrêt *Schlumpf c. Suisse*, 8 janvier 2009, §100.

exhaustive des aspects qui font partie de la vie privée. Cela fait du concept de vie privée une notion évolutive[16]. On trouve dans le paragraphe 2 de l'article 8 les trois fameuses conditions à remplir pour qu'une restriction puisse être posée au droit à la vie privée : la mesure doit être « *prévue par la loi* » (condition de légalité), et *« nécessaire, dans une société démocratique, à…* », ce qui exige l'existence d'un but légitime (condition de légitimité) tout en évitant que la mesure en question ne porte une atteinte trop forte aux droits et libertés de l'individu (condition de proportionnalité).

Au niveau de l'Union européenne, l'article 7 de la Charte des droits fondamentaux de l'Union européenne[17] offre un nouvel exemple de disposition législative qui protège le droit à la vie privée. La Charte expliquée fait elle-même le lien avec l'article 8 de la CEDH. Il en résulte que le régime juridique des restrictions à la vie privée, développé par la Cour EDH, est applicable de la même façon à l'article 7 de la CDFUE. On notera toutefois une légère évolution du terme « correspondances » qui a été remplacé par « communications », on s'en doute, pour mieux coller à la réalité technique des correspondances actuelles[18]. Depuis le Traité de Lisbonne (2009, la Charte a valeur de droit primaire en droit européen[19].

Enfin, on trouve également une disposition protégeant le droit à la vie privée dans le Pacte international relatif aux droits civils et politiques[20]. Son article 17 établit en effet une protection de la vie privée, mais va un pas plus loin que les protections de la Constitution et de la CEDH car il vise, en plus, l'honneur et la réputation[21].

Section 3. Lien entre vie privée et protection des données

On l'a vu, de nombreuses dispositions légales protègent le droit à la vie privée. Afin de pouvoir grimper la prochaine marche dans notre progression en escalier, il nous faut toutefois encore faire le lien entre ce droit et la protection des données personnelles. Dans son récent ouvrage de janvier 2019, « La vie privée à l'heure de la société du numérique », le professeur

[16] K. LEMMENS, *op. cit.,* p. 906.
[17] Art. 7 de la Charte des droits fondamentaux de l'Union européenne, adoptée à Nice le 7 décembre 2020.
[18] F. PICOD, C. RIZCALLAH, et S. VAN DROOGHENBROECK, « Annexe - La Charte des droits fondamentaux et ses explications publiées le 14 décembre 2007 », *Charte des droits fondamentaux de l'Union européenne*, Bruxelles, Bruylant, 2019, p. 1391.
[19] R. TINIÈRE, *op. cit.*, p. 30.
[20] Art. 17 du Pacte international relatif aux droits civils et politiques, fait à New York le 19 décembre 1966, approuvé par la loi du 15 mai 1981, *M.B.*, 6 juillet 1983.
[21] R. ERGEC, « Chapitre 5. – Droits concernant la vie privée et la vie familiale », *Convention européenne des droits de l'homme*, J. VELU et al. (dir.), 2e édition, Bruxelles, Bruylant, 2014, p. 652.

Yves Poullet nous explique ce lien par une fine analyse de la jurisprudence allemande. On comprend que « *(...) la juridiction constitutionnelle [allemande] déduit du droit à la personnalité le droit à l'autodétermination informationnelle (*Recht auf informationelle Selbstbestimmung[22]*), c'est-à-dire « le pouvoir reconnu à l'individu et résultant de la notion d'autodétermination, de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués »*[23]. Ce « droit à l'autodétermination informationnelle » concrétise en réalité un droit à la protection des données, né d'une mère « valeur de dignité » et d'un père « droit au développement de la personnalité » (qui n'est qu'une autre appellation pour désigner le droit à la vie privée), et a pris cette forme de manière à s'adapter aux nouvelles situations engendrées par le progrès de la technologie[24].

On l'a dit, l'autorité publique assume des obligations positives qui impliquent de protéger la vie privée du citoyen. Cela, combiné avec la dimension horizontale du droit à la vie privée, constitue, toujours selon Yves Poullet, « *les fondements de la consécration des régimes de protection des données à caractère personnel* »[25]. L'évolution des technologies de communication n'y est pas pour rien. En effet, celle-ci vient menacer le droit à l'autodétermination de l'individu vis-à-vis de ses concitoyens. S'il sait ses communications surveillées, il va lui-même se mettre des freins à son développement personnel. L'État, qui doit intervenir pour protéger ce développement de l'individu dans la société, en vertu de l'article 8 de la CEDH, va donc mettre en place les législations relatives à la protection des données, que l'on connait bien aujourd'hui. La Cour européenne des droits de l'homme a confirmé, à plusieurs reprises, que la communication de données relatives à la vie privée d'une personne constituait une ingérence dans le droit au respect de celle-ci[26]. La juridiction suprême de l'Union européenne a également fait état de conclusions dans ce sens[27]. Les deux notions de protection de la vie privée et de protection des données personnelles sont donc intimement liées. On le verra plus loin, distinguer les deux concepts de façon trop exclusive pourrait amener des risques.

---

[22] Droit qui avait déjà été affirmé par la Cour constitutionnelle allemande dans un arrêt de 1965 (BVerfGE, 65, I, pp. 43 et s.).
[23] Y. POULLET, *La vie privée à l'heure de la société du numérique*, 1e édition, Bruxelles, Larcier, 2019, p. 67.
[24] Y. POULLET, *ibidem*, p. 66.
[25] Y. POULLET, *ibidem*, p. 71.
[26] Cour eur. D.H., arrêt *Leander c. Suède*, 26 mars 1987, §48 ; Cour eur. D.H. (gde ch.), arrêt *Amann c. Suisse*, 16 février 2000, §69.
[27] CJCE, arrêt *Österreichischer Rundfunk*, 20 mai 2003, aff. jtes C-465/00, C-138/01 et C-139/01, EU:C:2003:294 ; CJCE, arrêt *Lindqvist*, 6 novembre 2003, C-101/01, EU:C:2003:596.

Chapitre III. Données personnelles

Maintenant que le lien a été fait entre vie privée et données personnelles, nous pouvons passer à la seconde marche de notre escalier et nous pencher sur la protection dont bénéficient nos données à caractère personnel. Il convient toutefois, avant cela, de définir correctement le concept de données personnelles, comme on a tenté de le faire avec la notion de vie privée (Section 1). On verra ensuite comment le droit protège ces données (Section 2). On terminera le chapitre par une réflexion visant à mettre en lumière les risques d'une distinction trop sévère entre vie privée d'un côté, et données personnelles de l'autre (Section 3).

Section 1. Définition des données à caractère personnel

Le Règlement général relatif à la protection des données à caractère personnel[28] (ci-après, « RGPD ») a été adopté le 27 avril 2016 et est applicable depuis le 25 mai 2018. On trouve, à son article 4, 1), une explication de ce que l'instrument comprend dans la définition de « données à caractère personnel ». Si l'on se cantonne à l'essentiel de la définition des « données à caractère personnel », on peut lire qu'elles sont donc « toute information se rapportant à une personne physique identifiée ou identifiable ». Si cette définition est courte, elle reste pour autant très large quant à son spectre.

En synthétisant fortement la doctrine qui s'est exprimée au sujet de cette définition, on peut finalement trouver une explication un peu plus précise. Il s'agirait de « toute donnée qui a une possibilité raisonnable d'être reliée à un individu en particulier ». On voit très vite qu'il faudra procéder à une analyse au cas par cas. Toutefois, le RGPD donne quelques exemples concrets de données à caractère personnel, qui le seront donc en tout temps : on citera, entre autres, un numéro d'identification, comme par exemple le numéro d'immatriculation d'une voiture, ou un identifiant en ligne, comme les identifiants universitaires des 30.000 étudiants de l'UCLouvain.

[28] Règlement (UE) 2016/679 (RGPD) du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016.

Section 2. Protection des données à caractère personnel

Évidemment, le RGPD ne se contente pas de définir la donnée à caractère personnel. Tout l'objet de cet instrument est de lui conférer une protection solide. On trouve la protection en question à l'article 6, §1 du RGPD[29]. La disposition ne rend le traitement de données à caractère personnel licite qu'à certaines conditions. Au premier rang de celles-ci, le consentement du sujet. C'est la condition la plus fréquemment rencontrée en pratique, car elle est facile à mettre en place pour le responsable du traitement des données.

Mais le RGPD ne se limite pas à encadrer le traitement des données à caractère personnel dans le chef du responsable du traitement. Il met également différents droits dans les mains du sujet de ces données. On peut mentionner un droit d'information[30], un droit d'accès[31], un droit de rectification[32], un droit à l'effacement (on parle souvent de « droit à l'oubli »)[33], un droit à la limitation du traitement[34], un droit à la portabilité des données (cela nous intéressera particulièrement dans le cadre de l'échange des données, *cf infra*)[35], un droit d'opposition[36] et un droit de ne pas faire l'objet de profilage (à retenir aussi pour la suite de l'exposé)[37].

Curieusement, on trouve dans la Charte des droits fondamentaux de l'Union européenne une disposition spécifiquement relative à la protection des données personnelles, juste après l'article 7, qui, pour rappel, offrait quant à lui une protection du droit à la vie privée. L'article 8 établit en effet un droit à la protection des données personnelles. Il présente lui-même ses modalités d'exercice : traitement loyal (d'où on pourrait souligner un rapprochement avec le *fair use* en droit intellectuel américain), conditions de consentement et/ou de légalité, droits du sujet, contrôle par une autorité indépendante[38]… Cette disposition présente comme avantages principaux d'une part le fait d'avoir apporté une certaine modernité à la CDFUE, quand on la compare avec d'autres instruments semblables qui, tout en protégeant eux aussi tout un panel de droits, ne sont pas à ce point en phase avec les évolutions technologiques d'aujourd'hui[39] et,

[29] Art. 6 du Règlement (UE) 2016/679 (RGPD).
[30] Art. 13 et 14 du Règlement (UE) 2016/679 (RGPD).
[31] Art. 15 du Règlement (UE) 2016/679 (RGPD).
[32] Art. 16 du Règlement (UE) 2016/679 (RGPD).
[33] Art. 17 du Règlement (UE) 2016/679 (RGPD).
[34] Art. 18 du Règlement (UE) 2016/679 (RGPD).
[35] Art. 20 du Règlement (UE) 2016/679 (RGPD).
[36] Art. 21 du Règlement (UE) 2016/679 (RGPD).
[37] Art. 22 du Règlement (UE) 2016/679 (RGPD).
[38] De façon similaire, l'article 51 du Règlement (UE) 2016/679 (RGPD) prévoit l'institution d'autorités publiques indépendantes chargées de surveiller son application dans les États membres.
[39] R. TINIÈRE, *op. cit.*, p. 31.

d'autre part, en ce qu'il renforce d'une certaine manière l'effectivité du droit à la protection des données personnelles[40].

Section 3. Risques d'une distinction trop stricte

Il ne faudrait toutefois pas surestimer ces deux apports. Comme le souligne Romain Tinière, l'article 8 de la CDFUE n'est que le « *prolongement de la Directive 95/46* » et du RGPD, sans qu'il n'ait apporté quelque nouvelle protection que ce soit, même au moment de sa rédaction, avant le RGPD[41]. L'auteur pousse donc à s'interroger sur la vraie valeur ajoutée du droit à la protection des données personnelles dans la CDFUE. En effet, la protection du droit à la vie privée, par le droit à l'auto-détermination informationnelle qu'elle comprend, suffit à elle seule à protéger les données à caractère personnel de l'individu[42]. Le risque, en voulant à tout prix rendre indépendante la protection des données personnelles par rapport à celle de la vie privée, serait d'en arriver à une dichotomie où la protection de la vie privée se traduit uniquement par les obligations négatives à charge de l'État et des tiers de ne pas entrer dans l'intimité de l'individu (« droit-bouclier »), tandis que la protection des données personnelles serait l'aspect « droit-épée » qui confère à ce même particulier des obligations positives à charge de l'État de lui garantir certains droits[43]. L'écueil à éviter est justement de penser qu'on peut séparer ces deux aspects. Ces deux-ci sont intimement liés et tous les deux nécessaires pour réaliser le droit à l'épanouissement, l'une des façons de concevoir le droit à la vie privée[44]. Quoi qu'il en soit, on ne pourra retirer le mérite de l'article 8 de la CDFUE d'avoir rendu ce droit plus visible[45].

[40] R. TINIÈRE, *ibidem*, p. 32.
[41] R. TINIÈRE, *ibidem*, p. 31.
[42] R. TINIÈRE, *ibidem*, p. 33.
[43] Y. POULLET, *La vie privée à l'heure de la société du numérique*, *op. cit.*, p. 74.
[44] Y. POULLET, *ibidem*, p. 75.
[45] R. TINIÈRE, *op. cit.*, p. 34.

Chapitre IV. Données personnelles sensibles

Nous arrivons enfin tout en haut de notre escalier. Cela nous mène au troisième niveau de protection qui s'applique aux données de santé. En effet, celles-ci constituent l'un des cas de « catégories particulières de données à caractère personnel ».

Section 1. Définition

En effet, le RGPD élève certaines données à caractère personnel au rang de catégories particulières de données personnelles. Selon l'alinéa 1er de l'article 9, il s'agit des « données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que (…) [les] données biométriques aux fins d'identifier une personne physique de manière unique, [les] données concernant la santé (…) [et les] données concernant la vie sexuelle ou l'orientation sexuelle d'une personne »[46]. Si l'on parle aujourd'hui de « catégories particulières de données personnelles », la notion est essentiellement la même que celle de « données sensibles » qui figurait dans la loi belge relative à la protection de la vie privée de 1992[47].

Section 2. Protection dans le RGPD

L'article 9 du RGPD va donc conférer à ces catégories particulières de données à caractère personnel une protection renforcée. Il va en effet prohiber en principe tout traitement qui concernerait celles-ci, sauf à remplir l'une des dix exceptions limitativement énumérées dans son second alinéa[48]. Parmi celles-ci, nous n'en citerons que cinq qui seront pertinentes pour l'analyse de l'échange des données relatives à la santé. Il s'agit du consentement explicite du sujet (a), les motifs d'intérêt public important (g), la nécessité à des fins médicales (h), la nécessité pour motifs d'intérêts publics importants dans le domaine de la santé publique (i) et la nécessité à des fins de recherche scientifique, historique ou de statistiques (j).

[46] Art. 9, §1er du Règlement (UE) 2016/679 (RGPD).
[47] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.
[48] Art. 9, §2 du Règlement (UE) 2016/679 (RGPD).

Notons encore que l'exception de nécessité à des fins médicales est renforcée par le troisième alinéa de l'article 9, qui précise que cette exception ne peut être mobilisée pour justifier le traitement de ces données que si ce traitement s'effectue sous la responsabilité d'un professionnel de la santé soumis à une obligation de secret professionnel[49].

Chapitre V. Conclusion sur la protection des données médicales

Les données relatives à notre santé sont donc clairement identifiées comme catégorie particulière de données personnelles par le RGPD[50]. Elles bénéficient de plusieurs autres niveaux de protection, certains inférieurs (protection de la vie privée et protection des données personnelles), mais ce qui compte finalement, c'est la protection supérieure dont elles bénéficient grâce au RGPD. Cela est dû au fait que les données relatives à notre santé ne recouvrent pas un simple aspect de notre vie privée comme un autre. La santé touche tellement à l'essence même de ce qu'est une personne physique vivante qu'il est naturel que toute information y relative fasse l'objet de la plus grande attention du législateur et soit en réalité si bien protégée.

Cela dit, ce n'est pas pour autant que les données relatives à notre santé ne doivent pas circuler. Comme nous le verrons dans le titre suivant, malgré la protection renforcée dont ces données font l'objet, une circulation de celles-ci reste possible et est même profitable, tant à l'individu, sujet de ces données, qu'à l'ensemble de la société.

[49] Art. 9, §3 du Règlement (UE) 2016/679 (RGPD).
[50] Voir également le considérant 35 du Règlement (UE) 2016/679 (RGPD).

Titre II. Échanges de données

Maintenant que l'on a vu l'intérêt, les raisons, l'obligation et les modalités de la protection des données médicales, il ne faudrait pas tomber dans le travers de se dire qu'il faut que nous conservions celles-ci à tout prix, sans envisager aucun flux de ces données si particulières. Comme on va bientôt le voir, l'échange des données relatives à la santé présente également certains enjeux non négligeables (Chapitre I). On verra ensuite comment le droit belge et le droit européen régulent ensemble l'échange de données publiques (Chapitre II), l'échange de données personnelles (Chapitre III) et l'échange de données non-personnelles (Chapitre IV). Sur base de tout cela, on terminera par une brève synthèse des opportunités qu'offrent les règles qui encadrent donc l'échange des données médicales (Chapitre V).

Chapitre I. Enjeux de l'échange des données de santé

Le professeur Alain Strowel, chargé de cours en faculté de droit de l'UCLouvain, fait souvent la comparaison entre les données et le pétrole. En effet, les données, et particulièrement les données personnelles, sont réellement le nouvel or noir du XXIe siècle, et la comparaison tient debout. Les données, comme le pétrole, doivent être « *proprement extraites, raffinées, transportées, stockées (…), puis estimées, vendues, utilisées* »[51]. Toutefois, le parallélisme s'arrête là. En effet, la donnée est une ressource différente du pétrole, en ce qu'elle constitue une donnée non-rivale[52], dans le sens où, quand elle a été utilisée une fois, elle garde toute sa valeur, au mieux elle en acquiert davantage. De plus, la quantité des données dans le monde est exponentielle, quand la quantité de pétrole encore disponible tend à se raréfier[53]. Les données, collectées et utilisées en grande quantité, vont donc présenter des enjeux majeurs, tant pour les intérêts généraux (leur compilation va permettre des statistiques impressionnantes, qui seront utilisées pour les politiques publiques, pour la recherche scientifique …) que pour les intérêts privés (les entreprises qui collectent les données peuvent également utiliser leur volume considérable, pour nourrir leurs systèmes d'intelligence artificielle (I.A.), pour améliorer leurs services…). Dans tous les cas, une bonne circulation des données pourra améliorer la

[51] A. STROWEL, L. SOMAINI, « The Regulation of Non-Personal Data in the EU and the 2020 Data Strategy », *Propriété intellectuelle à l'ère du Big Data et de la Blockchain*, J. DE WERRA (dir.), Zürich, Schulthess, 2020, p. 29
[52] A. STROWEL, L. SOMAINI, *ibidem*, p. 29.
[53] A. RAJAN, « Data is not the new oil », Réponse à *The Economist*, BBC News, 9 octobre 2017, http://www.bbc.com/news/entertainment-art-41559076, consulté le 21 avril 2021.

compétitivité des entreprises et donc la qualité de leurs services. L'Europe accuse d'ailleurs un lourd retard en matière d'IA par rapport aux États-Unis et à la Chine, ce qui accentue encore la nécessité d'une bonne circulation des données au niveau européen[54].

Ensuite, sur le plan de l'individu, du patient, l'échange des données relatives à sa santé va présenter une série d'avantages potentiels dans son chef. Une bonne circulation des données relatives à sa santé va avant tout permettre une meilleure prise en charge des soins de santé. Par exemple, si le professionnel a directement connaissance des allergies du patient, de ses maladies antérieures, il pourra mieux adapter sa prise en charge médicale. Aussi, cela va avoir une nette incidence sur les charges subies par le patient : si un examen médical avait déjà été réalisé antérieurement, et que le professionnel actuel a accès aux résultats de cet examen, il ne devra pas en prévoir un nouveau. Le patient peut aussi avoir beaucoup moins de formulaires à remplir si ses données sont sauvegardées et partagées dans un réseau auquel le personnel soignant a accès[55]. Le législateur, conscient de ces différents enjeux, a encadré le partage des différents types de données susceptibles de circuler.

Chapitre II. Échange de données publiques

Le principe de la publicité de l'administration[56], déjà mentionné *supra*, implique que l'autorité publique doit mettre à disposition de toute personne intéressée toute information dont elle dispose, et cela de façon gratuite[57]. Ce principe fait évidemment l'objet d'exceptions. C'est le cas si l'information requise à l'administration est confidentielle[58], porte atteinte à certains intérêts comme la sécurité de la population, les libertés et droits fondamentaux des administrés, l'ordre public, etc… [59], ou risque de violer le droit à la vie privée d'une autre personne si elle était communiquée[60]. Le citoyen bénéficie donc d'un certain droit d'accès aux données collectées par l'administration. En plus de cela, depuis 2016[61], il jouit également d'un droit à la

[54] C. VILLANI, *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, 8 mars 2018, p. 36.
[55] Règlement du partage de données de santé entre les systèmes de santé connectés via le répertoire de références de la plate-forme eHealth, approuvé par la délibération n° 14/016 du 18 février 2014 de la section santé du Comité sectoriel de la sécurité sociale et de la santé, pp. 3 et s.
[56] Const., art. 32.
[57] Loi du 11 avril 1994 relative à la publicité de l'administration, *M.B.*, 30 juin 1994.
[58] Loi du 11 avril 1994 relative à la publicité de l'administration, *M.B.*, 30 juin 1994, art. 6, §1er, 7° et 8° et §3, 2°.
[59] Loi du 11 avril 1994 relative à la publicité de l'administration, *M.B.*, 30 juin 1994, art. 6, §1er.
[60] Loi du 11 avril 1994 relative à la publicité de l'administration, *M.B.*, 30 juin 1994, art. 6, §2.
[61] Loi du 4 mai 2016 relative à la réutilisation des informations du secteur public, *M.B.*, 3 juin 2016.

réutilisation de ces données, à nouveau de façon gratuite, quand bien même la réutilisation serait destinée à des fins commerciales[62]. Cela implique que l'autorité publique à qui sont demandées les données doit les fournir gratuitement dans un format ouvert et lisible par machine[63].

L'Union européenne n'est pas en reste dans cette démarche de partage des données publiques. La directive ISP[64] (pour « informations du secteur public ») avait déjà initié le mouvement au niveau européen en 2003. Une étude commandée par l'UE constatait en 2017[65] que, malgré le cadre législatif qui a tendance à le favoriser, le flux des données des entreprises publiques n'était pas encore fort important. La Commission a proposé en 2018 de réviser cette directive, ce qui a donné naissance à la directive Open Data[66]. Quoiqu'il en soit, nous ne pouvons malheureusement creuser la question plus profondément, car l'échange des données publiques ne concerne pas les données relatives à la santé, sujet central de cette analyse.

Chapitre III. Échange de données personnelles

En ce qui concerne les données personnelles (qui sont, pour rappel, « toutes informations se rapportant à une personne physique identifiée ou identifiable »), on pourrait s'imaginer, à première vue, que leur circulation est extrêmement limitée du fait de la protection que le RGPD leur offre. Ce serait gravement se méprendre. En effet, le RGPD, au lieu de lutter contre l'échange des données personnelles, a ce double objectif de fond de protéger, d'une part, la vie privée du sujet des données, mais en même temps, de permettre une bonne circulation de ces données[67]. La directive 95/46[68], qu'il remplace, portait déjà ce double objectif[69]. Ce que fait concrètement le RGPD, c'est mettre entre les mains du sujet sa donnée, dès qu'elle sera

[62] A. DELFORGE, « L'accès et la réutilisation des données du secteur public : entre ouverture et protection des données à caractère personnel », *B.S.J.*, n° 621 (Janvier 2019-2), 2019, p. 14
[63] Loi du 4 mai 2016 relative à la réutilisation des informations du secteur public, *M.B.*, 3 juin 2016, art. 9, §2.
[64] Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *J.O.U.E.*, L 345, 31 décembre 2003.
[65] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Créer une économie européenne fondée sur les données », COM (2017) 9 final, 10 janvier 2017.
[66] Directive (UE) 2019/1024 du Parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, *J.O.U.E.*, L 172, 26 juin 2019.
[67] Art. 1er, §3 du Règlement (UE) 2016/679 (RGPD).
[68] Art. 1er de la Directive 65/46/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, *J.O.U.E.*, L 281, 23 novembre 1995.
[69] R. TINIÈRE, *op. cit.*, p. 31.

qualifiée de personnelle. Le sujet a des droits sur cette donnée (on ne parle toutefois pas encore d'un véritable droit de propriété). Parmi ceux-ci figurent notamment un droit d'accès (art. 15) et un droit à la portabilité (art. 20).

Le droit d'accès « *consacre le droit de la personne concernée d'accéder aux données traitées à son sujet et aux éléments qui entourent ce traitement (finalités du traitement, destinataires des données, etc.) mais aussi le droit d'en obtenir gratuitement une copie* »[70]. Le droit à la portabilité, quant à lui, implique que « *la personne concernée (…) a le droit de recevoir du responsable du traitement les données à caractère personnel qu'elle a fournies, dans un format structuré, couramment utilisé et lisible par machine, afin de transmettre ces données à un autre responsable du traitement* »[71]. Au travers de ce dernier droit particulièrement, on voit donc bien comment le RGPD permettra à terme un bon échange des données dès lors qu'il sera souhaité par le sujet de celles-ci.

De plus, le RGPD ne prohibe pas tout traitement des données à caractère personnel, loin de là. Il s'attache plutôt à l'encadrer pour protéger le sujet, mais dès le moment où celui-ci a donné son consentement au traitement de ses données personnelles, leur circulation peut reprendre. En définitive, si le sujet des données est celui qui en détient les clés, il peut toujours en autoriser l'utilisation. Le législateur a simplement mieux encadré ce processus d'autorisation, dans l'espoir de rendre le partage des données plus sûr, et donc à terme, de voir le citoyen y consentir plus aisément pour une meilleure circulation des données, qui reste un des objectifs de fond, sur le même pied que celui de protéger la partie faible (le sujet des données).

Chapitre IV. Échange de données non personnelles

Un troisième et dernier type de donnée mérite notre attention lors de l'analyse de l'échange des données. Il s'agit d'une catégorie située entre les données publiques et les données personnelles : les données non personnelles. Ces données non personnelles sont

[70] E. DEGRAVE, « Le R.G.P.D., les lois belges et le secteur public. Les traitements de données dans l'administration en réseaux et l'Autorité de protection des données », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, Limal, Anthemis, 2020, p. 290.
[71] C. DE TERWANGNE, « Présentation générale du R.G.P.D. et des lois belges relatives à la protection des données », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, Limal, Anthemis, 2020, p. 44.

longtemps restées non régulées. Toutefois, un règlement européen sur le libre flux des données à caractère personnel dans l'UE[72] est né en 2018, qui reposait sur une volonté de consacrer un principe de libre circulation des données.

La doctrine définit de manière négative les données non-personnelles par rapport aux données à caractère personnel. Il s'agit de « toute donnée ne se rapportant pas à une personne identifiée ou identifiable »[73]. La définition recouvre deux concepts, décrits par les lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne[74]. D'abord, on y trouve des données qui n'ont jamais concerné une personne physique identifiée ou identifiable. Il s'agit, par exemple, « *des données relatives aux conditions météorologiques générées par des capteurs installés sur des éoliennes ou les données relatives aux besoins de maintenance des machines industrielles* »[75]. Ensuite, cela concerne également « *les données qui étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues anonymes* »[76].

Mentionner la possibilité de rendre les données personnelles anonymes nous contraint à distinguer deux notions avant d'aller plus loin. L'article 4, §5 du RGPD définit la pseudonymisation comme étant « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[77]. L'anonymisation des données personnelles a cela de plus que la pseudonymisation que, en anonymisant les données, elle rendra impossible de relier celles-ci à une personne, quand bien même on utiliserait d'autres données stockées ailleurs[78].

[72] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *J.O.U.E.*, L 303, 28 novembre 2018.
[73] Article 2, §1er du Règlement (UE) 2018/1807.
[74] Communication de la Commission au Parlement européen et au Conseil, « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, COM (2019) 250 final, 29 mai 2019.
[75] J.-F. HENROTTE, « De la distinction entre l'anonymisation et la pseudonymisation », *J.L.M.B.* 2020, n°29, p. 1363.
[76] J.-F. HENROTTE, *ibidem*, p. 1363.
[77] Art. 5, §5, du Règlement (UE) 2016/679 (RGPD).
[78] J.-F. HENROTTE, *ibidem*, p. 1363.

On le voit, la frontière entre données personnelles et données non personnelles n'est pas fixe, et cela est dû en grande partie à la technologie, en constante évolution, qui permet d'identifier des personnes en recoupant différentes informations *a priori* anonymes[79]. La circulation de ces données, qui étaient auparavant des données personnelles, mais anonymisées par la suite, nous ouvre donc une porte pour le partage des données relatives à la santé aux fins de recherche (notamment).

Chapitre V. Conclusion sur l'échange des données médicales

Quel que soit le type de donnée concerné (publique, personnelle, non-personnelle), l'on voit que le législateur, souvent européen, a mis des instruments en place, certes pour baliser, mais avant tout pour rendre possible des échanges fluides et importants de ces données. La Commission européenne va jusqu'à mentionner la volonté d'instituer une « cinquième liberté fondamentale »[80].

[79] Romain Tinière, *op. cit.*, p. 29.

[80] Document de travail des services de la Commission sur la libre circulation des données et sur les questions émergentes sur l'économie européenne des données, accompagnant la Communication « Construire une économie européenne des données » (COM (2017) 9 final), SWD (2017) 2 final, 10 janvier 2017.

Partie II. Plateformes de données santé

Comme annoncé, cette seconde partie sera l'occasion d'aborder le fonctionnement de trois plateformes qui permettent actuellement, ou qui permettront dans un futur proche, la circulation des données de santé. La démarche se voudra descriptive et objective, de sorte à conserver l'analyse critique de ce fonctionnement pour la troisième partie de cette étude. Y seront donc détaillés, dans l'ordre, la plateforme gouvernementale « eHealth » (Titre I), la plateforme de Sciensano « healthdata.be » (Titre II) et un projet de l'Union européenne d'espace européen des données de santé (Titre III).

Titre I. La plateforme eHealth.be

Chapitre I. Description sommaire

La plateforme « eHealth »[81] (ou « eSanté ») est la plateforme de référence en Belgique en ce qui concerne l'échange des données de santé. Il s'agit de la plateforme du gouvernement qui va agir en tant qu'intermédiaire et convoyeur des données relatives à la santé des patients entre ces derniers et l'ensemble du système belge de soins de santé, d'une part, et entre les professionnels de la santé eux-mêmes, d'autre part. Elle se décline en effet entre ces deux volets.

Pour les patients, la première partie du site web[82] présente la principale utilité de leur donner accès au portail « Ma Santé », sur lequel ils peuvent retrouver une quantité d'informations relatives à leurs données de santé, ainsi qu'à leur circulation.

Pour les professionnels de la santé, la seconde partie du site[83] regroupe une longue série d'applications, portails, registres et services qui leur sont directement accessibles à cet endroit et qui présentent tous un lien avec l'enregistrement, la circulation ou la consultation de données relative à la santé des patients.

[81] « Page d'accueil | eHealth », https://www.ehealth.fgov.be/fr, consulté le 26 avril 2021.
[82] « Patients | eHealth », https://www.ehealth.fgov.be/fr/patients, consulté le 26 avril 2021.
[83] « Professionnels de la santé | eHealth », https://www.ehealth.fgov.be/fr/professionnels-de-la-sante, consulté le 26 avril 2021.

Chapitre II. Objectifs

Le Règlement[84] de la plateforme, approuvé en 2014, nous donne une bonne vision des différents objectifs que poursuit la plateforme. Comme on le verra, ils rappellent fortement les enjeux soulevés tant par la nécessité de la protection de la vie privée du patient que par l'intérêt du partage des données de santé, mentionnés *supra*.

La plateforme eHealth a pour **objectif final** de « *permettre l'interconnexion entre les systèmes régionaux et locaux d'échange d'informations relatives à la santé afin de permettre à un prestataire de soins de retrouver et de consulter les données électroniques relatives à la santé disponibles au sujet d'un patient et ce indépendamment, d'une part, du lieu effectif de stockage des données et, d'autre part, du point d'entrée du prestataire dans le système* »[85].

La plateforme porte évidemment un **objectif d'effectivité**, qui rejoint les enjeux du partage des données. S'il est effectif, le système permettra la réalisation des bénéfices que présente l'échange électronique de données personnelles relatives à la santé, à savoir principalement une prise en charge optimale du patient par le professionnel de la santé, qui bénéficiera dès lors de toutes les informations relatives à l'état de santé antérieur et actuel du patient (maladies, interventions chirurgicales, examens, allergies, prise de médicaments, soins prodigués…) et une nette diminution des charges, tant dans le chef du patient (qui ne devra plus subir qu'une seule fois certains examens, ne devra plus remplir qu'une seule fois certains formulaires…) que dans celui du médecin (prescriptions électroniques, attestations électroniques de soins…)[86].

La plateforme porte également un **objectif de légalité** qui, lui, rejoint les enjeux de la protection des données. Pour être utilisée et remplir son but final, la plateforme doit respecter les lois en vigueur qui concernent la protection de la vie privée. Et en effet, on lit dans le règlement que « *[l]ors de l'échange électronique de données de santé, une protection adéquate de la vie privée du patient et une sécurité de l'information solide sont évidemment essentielles* »[87].

[84] Règlement du partage de données de santé entre les systèmes de santé connectés via le répertoire de références de la plate-forme eHealth, approuvé par la délibération n° 14/016 du 18 février 2014 du Comité de sécurité de l'information (ci-après, « Règlement eHealth »).
[85] Règlement eHealth, p. 4.
[86] Règlement eHealth, p. 4.
[87] Règlement eHealth, p. 4.

En définitive, tout l'enjeu de la mise en place de la plateforme eHealth est de parvenir à un bon équilibre entre un échange de données efficace et la sécurité de l'information.

Chapitre III. Textes légaux et réglementaires

C'est la loi du 21 août 2008[88] qui a institué la plateforme eHealth et qui en fixe le cadre organisationnel.

Son règlement, souvent cité ici, reprend « *les règles communes minimales à respecter par l'organisation en vue de l'échange de données de santé entre les utilisateurs affiliés aux différents systèmes d'échange pour lesquels il est fait appel au répertoire des références de la plateforme eHealth* »[89]. Le règlement a été approuvé par la section santé du Comité sectoriel de la sécurité sociale et de la santé par une délibération n° 14/016 du 18 février 2014[90].

Les éléments relatifs à la manière par laquelle les patients donnent leur consentement à l'enregistrement de leurs données de santé dans le répertoire ont quant à eux été approuvés par la délibération n°12/047 du 19 juin 2012 de la section Santé du Comité sectoriel[91].

Il est enfin précisé que le Règlement tient compte d'autres lois en vigueur, notamment l'ancienne loi du 8 décembre 1992 relative à la vie privée[92] (aujourd'hui remplacée par le RGPD), la loi du 22 août 2002 relative aux droits du patient[93], ainsi que la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale[94].

[88] Loi du 21 août 2008 relative à l'institution et à l'organisation de la plateforme eHealth et portant diverses dispositions, *M.B.*, 13 octobre 2008.
[89] Règlement eHealth, p. 3.
[90] Délibération n°14/016 du Comité de sécurité de l'information portant sur le règlement du partage de données de santé entre les systèmes de santé connectés via le répertoire de références de la plateforme eHealth, CSI/CSSS/20/442, 18 février 2014.
[91] Délibération n° 12/047 du Comité de sécurité de l'information relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement, CSSSS/17/148, 19 juin 2012.
[92] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.
[93] Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 26 septembre 2002.
[94] 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.

Chapitre IV. Fonctionnement

Section 1. Architecture

La principale information à connaître à propos du fonctionnement de la plateforme eHealth est que celle-ci ne stocke pas les informations relatives à la santé des patients. C'est voulu, c'est d'ailleurs une des raisons qui justifient le choix posé d'adopter une approche décentralisée. Un autre avantage est que cela a permis de préserver les plateformes d'échanges et de stockage des données déjà présentes[95].

La plateforme eHealth ne stocke donc pas les données, elle les référence. À cette fin, un élément essentiel est le « répertoire des références ». Prévu par la loi du 21 août 2008[96], il est réellement ce qui constitue l'architecture du système d'échange. Celui-ci se constitue sur deux niveaux :

Au niveau centralisé (plateforme eHealth) se trouve un « *metahub* ». Ce *metahub* ne stocke aucune donnée, on l'a dit, et ne peut donc à lui seul fournir l'information recherchée sur la santé du patient. Son rôle est d'aiguiller la requête d'information en indiquant, si l'information sur la santé du patient existe, dans quel hub celle-ci se trouve.

Au niveau décentralisé, plusieurs « *hubs* » existent, qui sont des ensembles constitués regroupant différentes bases de données issues de structures de soins de santé. On peut citer, à titre d'exemple de *hub*, le « Réseau Santé Wallon », qui « *permet un échange de documents de santé informatisés (résultats d'examens, rapports médicaux, courriers, etc.) entre les prestataires de soins intervenant pour un même patient* »[97]. Le Réseau Santé Wallon regroupe par exemple différents hôpitaux tels que le CHU Ambroise Paré, le CHR Sambre et Meuse, le Centre hospitalier neurologique William Lennox, des cliniques comme la Clinique Saint-Luc de Bouge, la Clinique Reine-Astrid, des intercommunales telles que Vivalia… Le *hub* va avoir pratiquement la même fonction que le *metahub*, à savoir répertorier et organiser l'accès aux documents hébergés sur les serveurs des institutions qu'il englobe. Toutefois, il peut aussi directement servir de serveur lui-même pour héberger les données de santé collectées par

[95] Règlement eHealth, p. 5.
[96] Loi du 21 août 2008 relative à l'institution et à l'organisation de la plateforme eHealth et portant diverses dispositions, art. 5, 4°, b).
[97] « Réseau Santé Wallon – Qu'est-ce que c'est ? », https://www.reseausantewallon.be/FR/patients/Information/general-informations/Pages/generalities.aspx, consulté le 26 avril 2021.

certains acteurs de première ligne, comme le médecin généraliste, qui ne les stocke pas toujours lui-même sur un serveur.

Une nuance à apporter est que toutes les bases de données médicales en Belgique ne sont pas forcément affiliées à un *hub*. C'est pourquoi le *metahub* a également accès à deux autres « corps » : les « coffres-forts » de santé (tels que Vitalink) et les banques de données décentralisées (comme « Pharmaceutical Care Data Hub » qui héberge les Dossiers pharmaceutiques partagés). Sans donc passer par un *hub* intermédiaire, le *metahub* va directement référencer les données de santé présentes dans ces deux types de corps indépendants.

Il faut également préciser qu'au sein du *hub*, le patient est identifié par son numéro d'identification de la sécurité sociale (NISS)[98]. C'est donc par cet identifiant que la plateforme procédera à la recherche de référence dans le répertoire eHealth constitué par les *hubs* et le *metahub*.

A titre d'illustration, un médecin généraliste pourrait avoir besoin des résultats d'une radiographie du thorax que son patient X a subie une semaine plus tôt au CHR Haute-Senne. Ce médecin, pour obtenir cette information, va utiliser les services supportés par la plateforme eHealth. Sa requête, contenant le NISS du patient X, sera envoyée au *metahub* de la plateforme, qui sondera les différents *hubs* en cherchant la présence de données reliées à ce NISS. Il va trouver la présence d'une information dans le *hub* « Réseau Santé Wallon », qui va lui-même sonder les bases de données des différentes institutions qu'il regroupe. Comme le CHR Haute-Senne en fait partie, il confirmera la présence de l'info dans sa base de données et la plateforme eHealth aura ainsi établi le chemin vers la donnée relative à la santé du patient X que constitue l'imagerie de son thorax.

[98] Règlement eHealth, p. 5.

Section 2. Rôle du patient

Avant de montrer les applications concrètes que la plateforme eHealth peut fournir tant au patient qu'au médecin, il nous faut poser un préalable important. À l'issue de la description ici faite de l'architecture de la plateforme, un acteur pourrait sembler ne jouer qu'un rôle passif : il s'agit du patient. Or, il en est tout autrement.

En effet, le patient endosse au contraire un rôle-clé dans le jeu de l'échange des données relatives à sa santé. Le principe du consentement éclairé est la pierre angulaire du système. Le patient doit en effet avoir préalablement donné son consentement éclairé pour que ses données de santé soient référencées dans le répertoire et puissent être consultées[99]. Aussi, le patient jouit de certains droits, même après avoir donné son consentement, relativement à l'échange de ses données médicales.

§1. Consentement éclairé

L'exigence de consentement « éclairé » implique que la personne qui recueille le consentement ait correctement informé le patient sur la portée et les conséquences de cet acte.

Le Comité sectoriel a apporté une attention toute particulière à la manière dont était recueilli le consentement éclairé du patient. Une délibération spécifique a d'ailleurs été rendue sur le sujet[100]. À sa lecture, on comprend qu'on a voulu sécuriser au mieux le consentement du sujet. Ce dernier sera spécifiquement informé que l'échange de ses données de santé « *aura lieu d'une manière sécurisée et que la confidentialité et ses droits en tant que patient seront respectés* »[101].

§2. Enregistrement du consentement

C'est le patient lui-même (ou son représentant légal) qui peut enregistrer son consentement sur la plateforme eHealth. Cela se réalise matériellement par l'action de cocher une case « J'accepte » dès l'entrée sur le portail « Ma Santé » (la composante 'patient' de la plateforme eHealth, cf. *infra*). C'est donc un système d' « *opt-in* » qui a été choisi pour

[99] Règlement eHealth, p. 7.
[100] Délibération n° 12/047 du Comité de sécurité de l'information relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement, CSSSS/17/148, 19 juin 2012.
[101] Délibération n° 12/047 du Comité de sécurité de l'information relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement, CSSSS/17/148, 19 juin 2012, point 4.2, p. 2.

l'enregistrement du consentement[102]. L' « *opt-in* » implique que le fait de donner explicitement son consentement suffira pour le patient et qu'il ne lui sera pas demandé de signature.

Le consentement éclairé du patient peut également être enregistré par un médecin, un pharmacien, un infirmier, par les services administratifs d'un hôpital ou par une mutualité[103]. Dans ces cas-là, et pour confirmer qu'ils recueillent bien le consentement auprès du patient, l'enregistrement sera confirmé par la mention du numéro de sa carte d'identité. Cela se matérialise aujourd'hui de façon électronique, par l'introduction de la carte d'identité dans le lecteur de carte du prestataire (eID). Un document spécifique à signer peut toutefois remplacer cette procédure[104].

Une fois le consentement donné par le patient ou obtenu par le prestataire, celui-ci sera communiqué à la banque centrale des consentements de la plateforme eHealth. Cela permettra au patient de vérifier, par la suite, quel prestataire a participé à l'enregistrement de son consentement, ce qui met en œuvre son droit au retrait du consentement (*cf. infra*).

§3. Portée limitée du consentement

De plus, le consentement du patient a une portée limitée. Il ne vaut que pour les échanges de données approuvés par le Comité sectoriel de la sécurité sociale (**légalité de l'échange**), il ne permet qu'aux seuls prestataires de soins avec lesquels le patient concerné a effectivement une relation de soins d'accéder à ses données (**exigence d'une relation thérapeutique**), et il ne permet au prestataire de soins que d'accéder aux données de santé pertinentes pour le patient[105] (**principe de finalité**).

Il peut être opportun d'apporter quelques précisions relatives au second élément. Une relation thérapeutique peut se définir comme « *la relation entre un patient déterminé et un ou plusieurs professionnels des soins de santé associés à l'exécution des actes de diagnostic, de prévention ou de prestation de soins à l'égard du patient* ». Dans une note relative aux preuves électroniques d'une relation thérapeutique et d'une relation de soins[106], le Comité sectoriel (le

[102] Délibération n° 11/046 du Comité de sécurité de l'information relative à la note concernant le consentement éclairé dans le projet des hubs et du metahub, CSSS/14/080, 17 mai 2011.
[103] Règlement eHealth, p. 7.
[104] Règlement eHealth, p. 8.
[105] Délibération n° 12/047 du Comité de sécurité de l'information relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement, CSSSS/17/148, 19 juin 2012, point 4.2, p. 2.
[106] Délibération n° 11/088 du Comité de sécurité de l'information relative à la note relative aux preuves électroniques d'une relation thérapeutique et d'une relation de soins, CSSSS/11/134, 18 octobre 2011.

« Comité de sécurité de l'information » depuis 2018) consacre toute une analyse des modes de preuve de cette relation. Cela dépasse l'objet de notre analyse, mais contentons-nous de mentionner que la relation thérapeutique, en tant que condition à l'accès aux données de santé du patient par le prestataire de soins, est un élément factuel qui se prouve. C'est un élément qui, on le verra dans la partie III, renforce la protection de la vie privée du patient. Il ne faudrait donc pas sous-estimer cette exigence.

À l'inverse, il ne faudrait pas surestimer l'impact du troisième élément (le principe de finalité). Bien qu'il semble d'apparence limiter le traitement des données par le médecin, il a quand même été renseigné à ceux-ci de ne pas s'en inquiéter outre-mesure. En effet, « *dans le cadre des soins de santé, tous les renseignements personnels sont exploités à des fins de gestion du dossier médical de manière générale* »[107] peut-on lire dans un document de vulgarisation juridique à destination des dentistes. Il suffit donc au professionnel de la santé de rester dans les limites raisonnables d'une consultation des données à des fins générales de gestion du dossier médical.

§4. Droits du patient

Comme évoqué, une fois que le patient a donné son consentement éclairé pour l'échange de ses données médicales, il n'est pas pour autant privé de la gestion de celui-ci. Il peut en effet moduler son consentement sous plusieurs angles.

D'abord, parmi tout le flux de ses données de santé, le patient a la possibilité de demander que certaines de ses données ne soient pas échangées. Il peut également décider, sans devoir le justifier, que certains professionnels de soins de santé n'auront pas accès à ses données. Une telle exclusion ne peut être enregistrée dans la plateforme que par le patient, qui exclura alors nommément le prestataire dont il ne souhaite pas qu'il accède à ses données de santé. Le patient peut donc, en définitive, limiter l'échange des données tant à certaines données qu'à certains praticiens.

Ensuite, le patient bénéficie d'un droit de vision totale sur l'échange de ses données de santé. S'il a évidemment le droit de consulter ses données de santé lui-même, il peut aussi

[107] E. CAMBERLIN, T. DEFOUR, « RGPD : Conseils aux professionnels de la santé », https://www.dentiste.be/DocumentFromDatabase.aspx?id=205, consulté le 27 avril 2021, p. 2.

contrôler quel prestataire de soins de santé a accédé auxquelles de ses données de santé, et voir à quelle occasion cela s'est produit (via la date de consultation).

Last but not least, le patient a le droit de retirer son consentement à tout moment[108]. Grâce à l'enregistrement préalable de celui-ci, il pourra consulter à tout moment quel prestataire a procédé à l'enregistrement, et pourra retirer ce consentement si cela ne correspond pas à la réalité, ou sans aucune autre raison simplement s'il le souhaite.

§5. Exception : situation d'urgence

Il faut toutefois préciser que les deux conditions explicitées dans cette section peuvent être outrepassées légalement en cas d'urgence thérapeutique[109]. En effet, dans ce genre de cas, on ne vérifiera pas systématiquement l'existence du consentement éclairé du patient et d'une relation thérapeutique avec le prestataire qui prend le patient en charge (qui est justement souvent inexistante). Aussi, les exclusions ne valent plus dans ce type de situation exceptionnelle.

À des fins de contrôle, il sera toutefois enregistré dans les données de *logging* de la plateforme eHealth que le professionnel des soins de santé concerné a invoqué la situation d'urgence. Tout abus de cette exception peut donc être potentiellement sanctionné.

Section 3. Services / applications

En gardant bien tous ces principes en tête, on peut terminer l'analyse pratique de la plateforme eHealth en se rendant sur les portails web qu'elle fournit. Comme déjà évoqué, l'accueil du site se décline en deux volets : « Patients » (§1) et « Professionnels de la santé » (§2).

[108] Règlement eHealth, p. 8.
[109] Règlement eHealth, p. 10.

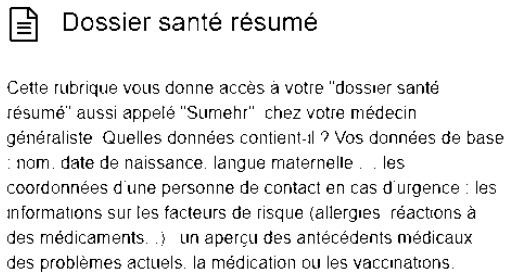
§1. Pour le patient

L'interface « Patients », outre le fait d'épingler quelques actualités à propos de la santé, présente le principal atout de mener directement au portail belge « Ma Santé »[110]. Également appelé « *Personal Health Viewer* », il agit comme point d'accès central pour la consultation, par le particulier, de diverses données à caractère personnel concernant sa santé, ou relatives à la santé en général. L'interface se présente en une série de zones, qui concernent chacune une application différente rendue possible par le partage des données de santé via la plateforme eHealth.

(Source des captures d'écran : www.ehealth.fgov.be)

Tout en haut de la liste figurent immanquablement deux onglets relatifs à l'épidémie de Covid-19. L'un concerne des données d'informations générales sur l'épidémie, mais l'autre mène vers les données personnelles du patient en lien avec le Covid-19 : ses résultats de test de dépistage, la possibilité de demander un certificat de quarantaine, de signaler un effet indésirable… Le citoyen belge trouvera également à cet endroit les différents moyens de prendre un rendez-vous pour se faire tester, ou pour se faire vacciner (après avoir reçu sa convocation).

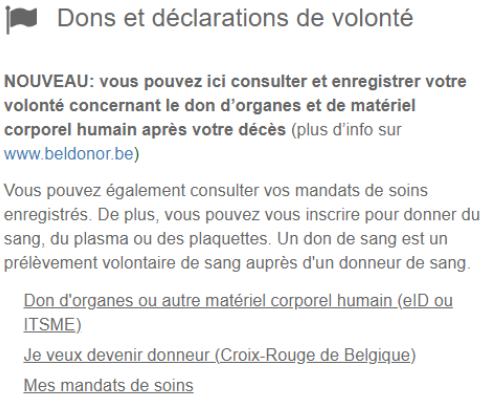
[110] « Ma Santé | eHealth », https://www.masante.belgique.be/#/, consulté le 27 avril 2021.



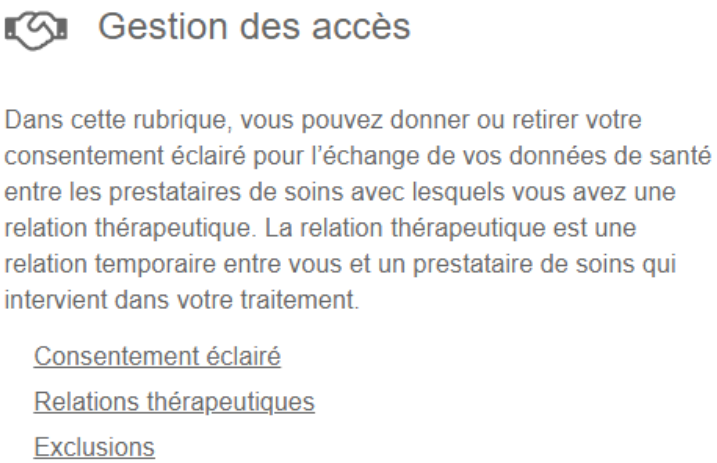
Un onglet important est l'onglet « *Sumehr* ». Il s'agit de l'accès au dossier santé résumé du patient. En cliquant dessus, il sera redirigé vers le portail web du hub auquel il est rattaché, en fonction des prestataires par lesquels il a été pris en charge. Un détour par le portail du Réseau Santé Wallon est donc indispensable dans ce survol :

Sur ce portail, après identification par eID (ou équivalent tel que « itsme® »), on peut accéder à tous les documents, rapports d'examens, d'interventions… nous concernant émis par les prestataires de soins de santé.

L'onglet « Dons et déclarations de volonté » permet quant à lui au patient de consulter l'état de son consentement au don d'organes et au prélèvement de matériel humain après son décès. Le cas échéant, c'est également via cette plateforme qu'il pourra le modifier : soit en le confirmant, soit en le retirant. En effet, le consentement au don d'organe est présumé par défaut pour le citoyen belge.



Mais l'onglet qui est probablement le plus pertinent dans cette analyse est celui qui concerne la gestion des accès. Via celui-ci, le patient pourra réellement mettre en œuvre les droits dont il bénéficie selon la protection de la vie privée et via le règlement de la plateforme eHealth.



Il a tout d'abord la possibilité de retirer (ou de redonner) son consentement éclairé à la plateforme eHealth. Retirer son consentement aura pour conséquence d'interrompre tout échange de ses données de santé, quel qu'il soit.

Le retrait du consentement est rendu très simple. Il s'agit d'un simple bouton « ON / OFF » qui ne requiert pas d'autre formalité pour être désactivé.

S'il souhaite plutôt nuancer cela, et ne pas pour autant s'opposer à la circulation de toutes ses données de santé entre tous les professionnels de soins, il pourra alors procéder aux exclusions qu'il souhaite. Ici également, le processus est rendu très simple. Le patient pourra soit encoder le numéro INAMI du professionnel à qui il souhaite restreindre l'accès à ses données, ou même simplement entrer son nom et son titre, s'il ne connaît pas le numéro INAMI du professionnel.

Un dernier onglet lui permet de consulter les relations thérapeutiques déclarées qu'il est supposé entretenir avec les professionnels de la santé : il y retrouvera, *a priori*, son médecin traitant, son dentiste, mais peut-être d'autres prestataires également, en fonction de sa situation particulière.

§2. Pour le professionnel de soins de santé

L'analyse de la partie du site de la plateforme eHealth dédiée aux professionnels de la santé[111] ne pourra pas aller aussi loin que celle de la partie conçue pour les particuliers, l'accès nous en étant restreint.

L'interface nous permet toutefois d'avoir un aperçu succinct des services en question. Il s'agit principalement d'un répertoire d'hyperliens menant à des applications à destination des médecins, soit directement accessibles via leur navigateur web… :

[111] « Services en ligne | eHealth », https://www.ehealth.fgov.be/fr/professionnels-de-la-sante, consulté le 27 avril 2021.

… soit accessibles via un logiciel médical :

On remarquera toutefois qu'il s'agit, pour la plupart de ces liens, d'accès à des services d'encodage, d'enregistrement, de déclaration… C'est en quelque sorte la « face cachée » de la plateforme eHealth. Car évidemment, pour qu'il y ait circulation des données de santé, il faut avant tout qu'il y ait un enregistrement de ces données qui soit réalisé en amont, et c'est ici que cela se passe.

En définitive, on voit bien le rôle d'intermédiaire que joue la plateforme eHealth. Bien plus un répertoire qu'un réel lieu de stockage, elle permet de bénéficier d'un point central pour accéder à une multitude de données éparpillées dans différentes bases de données aux quatre coins de la Belgique.

Mais le patient et le prestataire de soins ne sont pas les seuls qui à pouvoir tirer des bénéfices de ce référencement. Combiné à une autre plateforme, ce répertoire va présenter une seconde utilité, à un niveau beaucoup plus global…

Titre II. La plateforme healthdata.be

La plateforme eHealth permet donc de réaliser certains objectifs bénéfiques pour la relation entre le patient et le prestataire de soins, et entre prestataires eux-mêmes. Mais il ne s'agit pas des seuls enjeux que soulève la possibilité du partage des données relatives à la santé.

En effet, à un niveau beaucoup plus global, une autre plateforme belge d'échange de ces mêmes données de santé va permettre la réalisation d'une autre finalité : les statistiques, qu'elles soient destinées à des fins de recherche scientifique ou à des fins de soutien aux politiques publiques. La structure qui permet cela en Belgique est la plateforme « healthdata.be » de Sciensano, l'institution publique belge chargée des missions en matière de santé publique et animale[112].

La plateforme « healtdata.be » est « *un service technique qui a été développé (…) dans le but de « l'enregistrement, la conservation et la mise à disposition de données de santé et de soins de santé à des fins de recherche scientifique* »[113].

[112] « À propos de Sciensano | Sciensano.be », https://www.sciensano.be/fr/a-propos-de-sciensano, consulté le 28 avril 2021.
[113] « Dispositifs médicaux implantables et dispositifs médicaux de classe III », *B.I.-I.N.A.M.I.*, 2015/4, p. 74.

Chapitre I. L'organisme Sciensano

Sciensano est une institution publique, qui est née de la fusion entre le Centre d'Étude et de Recherches Vétérinaires et Agrochimiques (CERVA) et l'Institut scientifique de Santé publique (ISP), qui s'est produite en 2018. L'institution est donc récente. Elle revêt la qualité officielle d'organisme de recherche[114].

L'organisme a pour mission principale de guider la politique publique de santé de sorte à garantir au mieux à tout individu, quel que soit son âge, « une vie en bonne santé ». Pour ce faire, il concentre ses activités scientifiques sur six domaines d'action : la santé et l'environnement, la consommation et la sécurité alimentaires, la surveillance de la santé et des maladies, la qualité des soins de santé, la santé animale, et l'efficacité et la sécurité des vaccins, des médicaments et des produits de santé. Elle agit à tous les niveaux : fédéral, régional, communautaire, européen et international.[115] C'est principalement dans le domaine de la surveillance de la santé et des maladies qu'elle a mis en place la plateforme healthdata.be, que nous allons analyser ci-après.

Chapitre II. Textes légaux et réglementaires

L'institution Sciensano a été créée par la loi du 25 février 2018[116].

La plateforme healthdata.be a été conçue dans le cadre de l'accord de collaboration entre l'INAMI et l'ISP. Ce projet s'inscrit dans le cadre du Plan d'action e-Santé 2013-2018[117].

[114] Depuis son agréation par la Politique scientifique fédérale.
[115] « À propos de Sciensano | Sciensano.be », https://www.sciensano.be/fr/a-propos-de-sciensano, consulté le 28 avril 2021.
[116] Loi du 25 février 2018 portant création de Sciensano, *M.B.*, 21 mars 2018.
[117] « Plan d'action e-Santé 2013-2018 », *M.B.* 31/1, https://www.absym-bvas.be/fr/lois/2014-20140909111134, consulté le 28 avril 2021.

Chapitre III. Objectifs de la plateforme

La plateforme healthdata.be vise concrètement à « *permettre la réutilisation d'informations digitalisées venant de professionnels de la santé ou de bases de données agréées à des fins de recherche* »[118]. Ce **but final** se décline en plusieurs sous-objectifs.

Elle porte d'abord un **objectif de répertoriage**. En effet, on l'a vu, toutes les données de santé des citoyens belges restent dispersées dans une quantité assez élevée de bases de données à travers tout le pays. À ce titre-là, la plateforme eHealth organise déjà un solide répertoire des références. Mais les données de santé des patients ne sont pas les seules qui intéressent les statistiques. Les données de facturation, ou les données cliniques par exemple, présentent le même intérêt. C'est donc dans cette dimension-là que Sciensano est aujourd'hui parvenu à répertorier plus de 150 bases de données de santé. Son site annexe « healthstat.be » liste ces bases de données en proposant, à côté de chacune d'elle, une description, ses principaux objectifs, les spécialités médicales concernées, le type d'informations qu'on y retrouve…[119].

La plateforme healthdata.be présente ensuite **l'objectif de dynamiser la recherche**. Par ses services, elle va tendre à « *standardiser et homogénéiser l'enregistrement et la conservation des données de santé* »[120], et cela dans le but ultime de leur diffusion à des fins de recherche. Le projet se targue, sur son site web, de contribuer largement au « *déploiement d'une infrastructure-système dédiée à la recherche en Belgique* »[121].

Évidemment, la plateforme affiche également un **objectif de protection de la vie privée**. Elle tient à rassurer le sujet en lui expliquant que ses données ne seront communiquées qu'à des chercheurs, et ce dans cet unique but précis d'amélioration de la qualité et de la gestion des soins de santé (comprenant la recherche scientifique, le suivi sanitaire et l'approfondissement continu des connaissances)[122]. Il est également fait mention du fait que les données sont transmises à la recherche de manière agrégée et codée. On reviendra sur ce point dans l'analyse du fonctionnement de la plateforme (cf. *infra*).

---

[118] F. DE VISSCHER *et al.,* « Rights in data », *Ing.-Cons.,* 2020/2, Bruxelles, Larcier, 2020, p. 390.
[119] https://healthdata.sciensano.be/fr/%C3%A1-propos-healthdatabe
[120] « À propos de Sciensano | Sciensano.be », https://www.sciensano.be/fr/a-propos-de-sciensano, consulté le 28 avril 2021.
[121] *Ibidem*.
[122] *Ibidem*.

À terme, et dans le cadre du Protocole d'accord BelRAI[123], la plateforme healthdata.be a contribué à la création d'un grand « *data warehouse* », une immense base de données appelée « BelRAI », qui elle-même contribue à la réalisation d'objectifs de la politique de santé publique : optimalisation de la qualité et de la continuité des soins, simplification des procédures, optimalisation des décisions de remboursement de l'INAMI…[124]. BelRAI doit également viser la mise à disposition d'un set de données aux fins de recherches[125]. Enfin, l'instrument a également pour objectif de promouvoir les échanges électroniques de données de façon sécurisée, avec les garanties suffisantes en matière de protection de la vie privée[126].

Chapitre IV. Fonctionnement de la plateforme

Concrètement, la plateforme healthdata.be de Sciensano fonctionne au travers de deux services : d'une part, la collecte des données (Section 1) et d'autre part la fourniture des données (Section 2).

Section 1. Collecte de données

La plateforme va tout d'abord devoir collecter les données de santé auprès des différentes bases de données. Ces données, on l'a dit, restent éparpillées dans une multitude de bases de données au travers du Royaume. Heureusement, il existe un outil, que l'on a déjà vu, qui répertorie et référence l'existence et la localisation de toutes ces données : la plateforme eHealth.

Une application développée par Sciensano, dans le cadre de cette collecte de données, appelée « HD4DP » (pour « *Health Data for Data Providers* »), va utiliser la boîte eHealth pour trouver les chemins vers les emplacements dans les bases de données des institutions qui l'ont installée sur leurs terminaux. L'application HD4DP va lancer un processus de collecte (« *collection process* ») qui va transférer toutes les données à Sciensano[127].

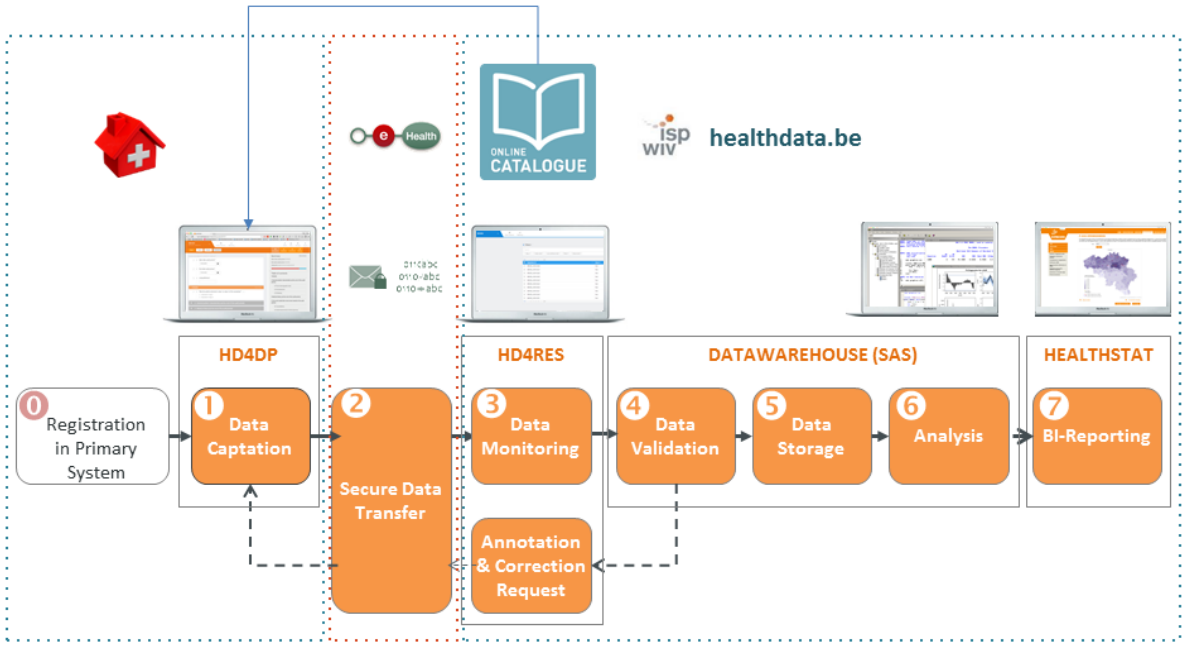
---

[123] Protocole d'accord du 26 mars 2018 conclu entre le Gouvernement fédéral et les Autorités visées aux articles 128, 130, 135 et 138 de la Constitution, décrivant la collaboration entre les parties signataires en vue de l'utilisation de l'instrument BelRAI, *M.B.,* 4 juin 2018 (ci-après, « Protocole d'accord BelRAI »).
[124] Protocole d'accord BelRAI, art. 1er, §1er, a, c et g.
[125] Protocole d'accord BelRAI, art. 1er, §1er, f.
[126] Protocole d'accord BelRAI, art. 1er, §1er, e.
[127] « Un aperçu de l'application HD4DP », https://support.healthdata.be/articles/fr/Support_Article/An-overview-of-the-HD4DP-application/, consulté le 28 avril 2021.

Toutefois, Sciensano ne va pas recevoir les données de santé telles qu'elles figurent dans la base de données de l'institution d'où elles proviennent. Par exemple, Sciensano ne recevra pas l'info comme quoi le patient X (avec le NISS xxxxxx-xxx-xx) a été diagnostiqué comme porteur d'une tumeur aux poumons.

Non, le secret médical et professionnel va être protégé pendant le processus, *« à différents niveaux et à travers des principes tels que l'encodage, le cryptage et la gestion des utilisateurs* », dont la combinaison « *garantit la sécurité de bout en bout* »[128]. Le patient est donc « désidentifié et réidentifié » par un identifiant codé. En plus de cela, les données seront anonymisées et agrégées, de telle sorte qu'au terme du processus de collecte, la plateforme de Sciensano recevra alors l'information comme quoi, par exemple, au cours de la semaine écoulée, 12 patients masculins âgés de plus de 60 ans ont été diagnostiqués porteurs d'une tumeur aux poumons.

De la sorte, explique Sciensano sur son site web, « *le fournisseur de données ne reçoit jamais les identifiants codés ; eHealth n'a jamais accès aux données médicales ou aux métadonnées ; healthdata.be ne reçoit jamais l'identifiant original, mais peut concilier différentes entrées* »[129].



(source : https://healthdata.sciensano.be/fr/services) .

[128] *Ibidem.*
[129] *Ibidem.*

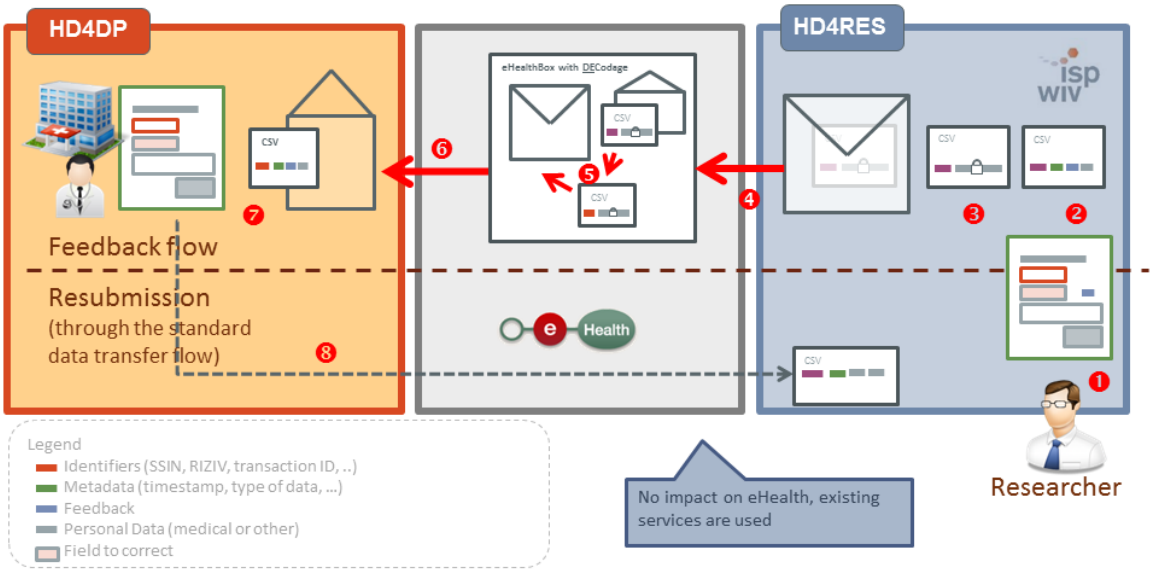
Section 2. Fourniture de données

Une fois ces données ainsi collectées et anonymisées au sein de son *data warehouse* « BelRAI », la plateforme healthdata.be va proposer un second type de service : il s'agit de la mise à disposition de toutes ces données pseudonymisées. Ce service s'adresse aux institutions scientifiques, aux associations professionnelles, ainsi qu'à d'autres personnes morales de droit privé et de personnes physiques.

Dans ce cadre-là, une deuxième application a été mise au point par Sciensano, qui s'appelle « HD4RES » (pour « *Healthdata for Researchers* »). Elle est « *une application web qui permet au chercheur de contrôler le flux de données, et si nécessaire, pour communiquer avec les fournisseurs de données sur la qualité des données, d'une manière uniforme et sécurisée* »[130]. Via cet environnement, le chercheur peut formuler une demande de données de santé, suivre le statut de leur collecte, y recevoir précisément les données dans un format CSV, et contrôler celles-ci.

Comme déjà expliqué, la demande va transiter via la plateforme eHealth, au moyen de l'eHealthBox-codage. Le chercheur recevra toutes les données demandées de manière codée, anonymisée et agrégée, de telle sorte qu'il lui est impossible de rattacher l'une de ces données à un patient en particulier. Comme le service lui permet également de contrôler les données et, si elles ne sont pas complètes ou s'il ne les comprend pas, de poser des questions au fournisseur de données, cette demande impliquera que les données collectées fassent le trajet retour vers l'expéditeur. Comme à l'aller, elles passeront par l'eHealthBox codage, qui décodera les données, pour permettre au fournisseur de données de rendre un feedback éclairé sur des données que lui pourra comprendre, qu'il joindra aux données qui referont une dernière fois le trajet inverse, toujours via l'eHealthBox, pour revenir en format codé au chercheur.

[130] « HD4RES | healtdata.be », https://healthdata.sciensano.be/fr/hd4res, consulté le 28 avril 2021.



(source : https://healthdata.sciensano.be/fr/services) .

Le service est gratuit pour les institutions publiques. Pour les autres demandeurs de données, « *un coût est facturé qui concerne les prestations effectives pour a) l'analyse fonctionnelle de la demande, b) la gestion du dossier (y compris la procédure d'obtention d'autorisation du Comité sectoriel et le dossier unique eHealth), c) la constitution de l'ensemble de données, d) la gestion des utilisateurs et des accès et e) l'espace de stockage des données. Le coût ne porte nullement sur les données proprement dites* »[131].

Section 3. Applications concrètes

Depuis son lancement en 2014, la plateforme healthdata.be fournit des compilations de données de santé à une grande quantité d'institutions, de centres de recherches, de registres, de réseaux de surveillance… Tous ces projets ont été initialement prévus par vagues, au nombre de trois. La troisième vague a été implémentée en 2016-2017, mais de nouveaux projets viennent toujours actuellement agrandir le nombre de bénéficiaires des données collectées par la plateforme.

Pour n'en citer que quelques-uns, on y trouve par exemple, au niveau régional, les déclarations de maladies infectieuses en Région wallonne ; au niveau national, le Registre belge des maladies neuromusculaires ou la Surveillance belge SIDA-VIH ; au niveau européen, le réseau européen Surveillance de consommation d'antimicrobiens.

[131] « Services | healthdata.be », https://healthdata.sciensano.be/fr/services, consulté le 28 avril 2021.

Titre III. Le projet d'espace européen des données santé

Une troisième plateforme mérite notre attention dans cette analyse de l'échange des données de santé. En effet, l'Union européenne s'est montrée particulièrement prolifique en matière d'initiatives numériques ces trois dernières années. L'une d'elles pourrait bien venir prochainement compléter le tableau des plateformes de circulation des données de santé.

Chapitre I. Le contexte politique

Section 1. La Commission Junker (2014-2019)

La précédente Commission européenne avait déjà montré la volonté de renforcer la numérisation dans le secteur sanitaire. Sa communication du 25 avril 2018 sur la transformation numérique des services de santé et de soins[132], plus communément appelée « Communication eHealth », repose sur trois piliers : mettre en place un accès sécurisé aux données et un partage sécurisé de ces données, connecter et partager des données de santé à des fins de recherche, de diagnostic plus rapide et d'amélioration de la santé, et renforcer l'autonomisation des citoyens et les soins individuels grâce aux services numériques[133].

On note donc déjà en 2018 cette intention de mettre en place des infrastructures qui permettront des échanges performants de données de santé entre professionnels de la santé. On voit dans le premier pilier que l'objectif à court terme était, déjà à l'époque, que ceux-ci puissent s'échanger facilement les dossiers de patients et des ordonnances électroniques. Un objectif à long terme visait, quant à lui, à mettre en place un format européen d'échanges de dossiers santé informatisés qui seraient accessibles à tous les citoyens européens[134]. Le deuxième pilier annonce encore plus visiblement le but de la Commission d'exploiter le potentiel que représentent les données de santé agrégées pour la recherche scientifique[135].

[132] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Permettre la transformation numérique des services de santé et de soins dans le marché unique numérique ; donner aux citoyens les moyens d'agir et construire une société plus saine », COM (2018) 233 final, 25 avril 2018 (ci-après, « Communication eHealth »).
[133] « Santé en ligne », https://ec.europa.eu/health/ehealth/home_fr, consulté le 29 avril 2021.
[134] Communication eHealth, p. 6.
[135] Communication eHealth, p. 12.

Section 2. La Commission von der Leyen (2019-2024)

Dans son programme pour l'Europe, Ursula von der Leyen, alors candidate à la présidence de la Commission européenne, fixait six orientations politiques[136] pour la prochaine Commission européenne. Depuis sa nomination à la présidence de la Commission, l'institution a fait de ces orientations ses six priorités pour la période 2019-2024[137]. L'une de ces six priorités est l'initiative européenne pour « *une Europe adaptée à l'ère numérique* ». Elle vise à « *permettre aux citoyens de disposer d'une nouvelle génération de technologies* »[138].

Dans une volonté de renforcer sa souveraineté numérique[139], une attention toute particulière est consacrée aux données, aux technologies et aux infrastructures. L'Union vise donc réellement à façonner l'avenir numérique de l'Europe. Trois piliers sont identifiés pour soutenir cette stratégie : la technologie au service des personnes, une économie numérique juste et compétitive, et une société ouverte, démocratique et durable. C'est au titre de ce dernier pilier que la Commission a annoncé que « *[sa] stratégie numérique (…) créera un espace européen des données de santé afin de promouvoir une recherche, des diagnostics et des traitements ciblés* »[140].

D'après la Commission, *« des dossiers médicaux numérisés, rassemblés dans un espace européen des données relatives à la santé, peuvent permettre un traitement plus efficace des principales maladies chroniques, y compris le cancer et des maladies rares, mais aussi l'égalité d'accès à des services de santé de qualité pour tous les citoyens* »[141]. La Commission, dans sa stratégie pour façonner l'avenir numérique de l'Europe, va jusqu'à donner des actions-clés pour parvenir à la réalisation de ces objectifs. Pour permettre cet échange de dossiers médicaux, elle compte agir dans le sens de « *La promotion des dossiers médicaux électroniques fondés sur un*

---

[136] À savoir : un pacte vert pour l'Europe, une économie au service des personnes, une Europe adaptée à l'ère du numérique, la protection du mode de vie européen, une Europe plus forte sur la scène internationale, et un nouvel élan pour la démocratie européenne.

[137] U. VON DER LEYEN, *Une Union plus ambitieuse. Mon programme pour l'Europe - Orientations politiques pour la prochaine Commission européenne 2019-2024*, 16 juillet 2019, p. 5.

[138] « Les priorités de la Commission européenne | Commission européenne », https://ec.europa.eu/info/strategy/priorities-2019-2024_fr#priorities, consulté le 29 avril 2021.

[139] « Une Europe adaptée à l'ère numérique | Commission européenne », https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_fr, consulté le 29 avril 2021.

[140] « Façonner l'avenir numérique de l'Europe | Commission européenne », https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_fr, consulté le 29 avril 2021.

[141] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Façonner l'avenir numérique de l'Europe », COM (2020) 67 final, 19 février 2020, p. 13.

format d'échange européen commun, afin que les citoyens européens puissent accéder aux données relatives à leur santé et les communiquer de manière sécurisée dans l'ensemble de l'UE. Un espace européen des données de santé destiné à améliorer la sécurité et la sûreté de l'accès aux données de santé, qui permettra de mieux cibler et d'accélérer la recherche, le diagnostic et le traitement (à partir de 2022) »[142].

Chapitre II. Le projet d'espace européen des données de santé

La Commission veut concevoir cet espace européen des données de santé sur « *des bases transparentes* », de façon à « *protéger pleinement les données des citoyens et à renforcer la portabilité de leurs données de santé* »[143].

L'objectif final consiste concrètement à « *améliorer les échanges et l'accès à différents types de données sur la santé (dossiers médicaux électroniques, données génomiques, données issues de registres de patients, etc.)* »[144]. Ces échanges, quand ils seront optimalisés, pourront d'une part « *soutenir la fourniture de soins de santé* »[145] (c'est l'utilisation « primaire » des données) et, d'autre part, « *soutenir la recherche sur la santé et l'élaboration de politiques en la matière* »[146] (il s'agit là de l'utilisation « secondaire » des données).

Une proposition de règlement est prévue pour le dernier trimestre 2021[147]. En attendant, la Commission a à nouveau identifié trois piliers généraux qui serviront d' « action commune » pour soutenir l'espace européen des données de santé.

Tout d'abord, la Commission devra assurer la mise en place d'un système solide de gouvernance des données. Autant pour l'utilisation primaire que pour l'utilisation secondaire des données, un cadre de règles devra être mis en place. À cette fin, une étude sera conduite sur la manière dont les différents États membres ont implémenté les règles du RGPD dans leur secteur des soins de santé, de façon à examiner par quelles modalités techniques ceux-ci parviennent, ou non, à garantir la protection de la vie privée des patients tout en maintenant un

[142] *Ibidem*, p. 14.
[143] « European Health Data Space | Santé publique », https://ec.europa.eu/health/ehealth/dataspace_fr, consulté le 29 avril 2021.
[144] *Ibidem*.
[145] *Ibidem*.
[146] *Ibidem*.
[147] « Données et services numériques en matière de santé – L'espace européen des données de santé », https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-A-European-Health-Data-Space-, consulté le 29 avril 2021.

trafic constant des données relatives à leur santé. Dans le prolongement de cela, l'étude devra aussi faire ressortir une « *vue d'ensemble des structures de gouvernance existantes pour l'utilisation secondaire des données de santé dans les pays de l'UE* »[148]. On le devine, en ce qui concerne la Belgique, c'est le schéma de gouvernance de Sciensano qui apparaîtra dans cette étude, vu que c'est l'organisme qui réalise ce que l'UE appelle « l'utilisation secondaire des données de santé ». Au terme de l'étude, la Commission espère tirer des recommandations d'actions (législatives ou non) qu'il serait possible de mener à l'échelon européen de sorte à « *faciliter le partage de données de santé dans l'ensemble de l'UE pour les utilisations primaires et secondaires* ».

Ensuite, l'UE veut mettre le focus sur les données elles-mêmes. D'une part, les données devront afficher un certain niveau de qualité. En effet, un agglomérat de données incomplètes, ou qui ne seraient plus à jour, nuirait grandement au projet et ne permettrait pas d'exploiter pleinement le potentiel des échanges de données de santé. D'autre part, les données devront également afficher un certain niveau d'interopérabilité. Il est nécessaire que les différentes bases de données soient capables de communiquer entre elles. Il faudra pour ça implémenter « *une interopérabilité technique et sémantique entre les différents systèmes informatiques et infrastructures* »[149]. Dans ce cadre, la Commission encourage à la « FAIR-ification » des sources de données existantes. Le concept de « FAIR-ification » recouvre l'idée d'attacher aux données stockées quatre qualités : elles doivent être faciles (à trouver), accessibles, interopérables et réutilisables[150].

Enfin, il faudra développer, au niveau européen, des infrastructures solides et interopérables. Celles-ci devront être adaptées aux spécificités du secteur de la santé, s'appuieront sur des structures déjà existantes (telles que l'infrastructure de services numériques dans le domaine de la santé en ligne, les réseaux européens de référence, ou le projet génomique) mais, de manière générale, « *suivront la stratégie globale de l'espace européen des données lancée par la publication de la stratégie européenne pour les données* »[151]. Cette indication nous offre l'occasion de nous pencher quelques instants sur cette stratégie globale en prenant un peu de hauteur par rapport aux données de santé.

---

[148] « European Health Data Space | Santé publique », https://ec.europa.eu/health/ehealth/dataspace_fr, consulté le 29 avril 2021.
[149] *Ibidem*.
[150] *Ibidem*.
[151] *Ibidem*.

Chapitre III. La stratégie globale d'espace européen des données

Consciente des multiples enjeux que soulèvent les données en général, l'Union ne se cantonne bien sûr pas à promouvoir l'échange de données de santé. C'est bien plus que cela, car elle vise réellement à atteindre une économie fondée sur les données, un marché unique européen des données[152].

Dans sa volonté de rendre les données les plus accessibles pour leur réutilisation, la Commission a dévoilé à la fin de l'année 2020 sa stratégie globale pour les données[153]. Après avoir rappelé les instruments déjà existants en matière de données (le RGPD en 2016, le règlement sur le flux des données non personnelles de 2018, le règlement sur la cybersécurité de 2019, et la directive OpenData de 2019), elle liste les aspects techniques à privilégier pour rencontrer ses objectifs. Pour les citer de manière synthétique, il s'agit de renforcer le traitement et le stockage des données, la connectivité des bases de données, d'augmenter la puissance de calculs effectués sur base des données, et d'assurer un bon niveau de cybersécurité[154]. L'Union devra également « *améliorer ses structures de gouvernance des systèmes d'échanges de données et, enfin, augmenter ses réserves communes de données* »[155]. À noter également que la Commission va rappeler sa vision globale, qui est de maintenir l'être humain au centre en respectant les valeurs et droits fondamentaux de l'Union[156].

Consciente qu'il va dès lors falloir évoluer de manière cohérente sur deux tableaux à la fois (permettre un meilleur accès aux données tout en fixant un cadre qui assure une utilisation responsable de celles-ci[157]), la Commission va faire évoluer son objectif de fond de créer un espace européen unique des données selon une stratégie qui repose sur quatre piliers.

Il s'agira, premièrement, de mettre en place un « *cadre transsectoriel de* ***gouvernance*** *pour l'accès et l'utilisation des données* »[158]. Comme action concrète, la Commission prévoyait principalement de proposer un cadre législatif pour la gouvernance des espaces européens

[152] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM (2020) 66 final, 19 février 2020, p. 6.
[153] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM (2020) 66 final, 19 février 2020.
[154] *Ibidem*, p. 2.
[155] *Ibidem*, p. 2.
[156] *Ibidem*, p. 6.
[157] *Ibidem*, p. 6.
[158] *Ibidem*, p. 15.

communs des données, prévu pour le dernier trimestre 2020. La Commission suit son planning, car elle a effectivement déposé le 25 novembre 2020 une proposition de règlement au Parlement européen sur la gouvernance européenne des données[159]. Il était également prévu d'adopter un acte d'exécution concernant les ensembles de données à haute valeur ainsi que de proposer une loi sur les données. Ces deux dernières initiatives devraient voir le jour cette année[160].

Deuxièmement, la Commission prévoit de solides « ***investissements*** *dans les données, et pour renforcer les capacités et les infrastructures européennes pour l'hébergement, le traitement et l'utilisation des données, tout en garantissant leur interopérabilité* »[161]. En termes de chiffres, elle prévoit un investissement total de 4 à 6 milliards d'euros pour ce levier, financé en partie par la Commission elle-même (à hauteur de 2 milliards, en fonction du budget européen), et en partie par les États membres et l'industrie (à hauteur de 2 à 4 milliards)[162]. Ces investissements auront principalement lieu pour un « *projet à forte incidence relatif aux espaces européens de données* »[163], projet qui constitue le quatrième pilier de sa stratégie (cf. *infra*).

En troisième lieu, l'exécutif européen prévoit de travailler sur les **compétences** à tous les niveaux. Ce pilier vise à « *donner à chacun les moyens d'agir en ce qui concerne ses données et investir dans les compétences et dans les PME* »[164]. À ce titre, l'institution a prévu comme action-clé d' « *étudier la possibilité de renforcer le droit à la portabilité pour les personnes physiques au titre de l'article 20 du RGPD, en leur permettant de mieux contrôler qui peut accéder aux données générées par des machines et les utiliser* »[165]. Elle précise que cela pourrait se produire à l'occasion de la nouvelle loi sur les données annoncée pour 2021 dans le premier pilier.

Quatrièmement, la Commission annonce la création d'**espaces européens** communs des données dans des secteurs stratégiques et des domaines d'intérêt public[166]. On le devine, c'est

[159] Communication de la Commission portant proposition de règlement du Parlement européen et du Conseil sur la gouvernance des données, COM (2020) 767 final, 25 novembre 2020.
[160] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM (2020) 66 final, 19 février 2020, p. 19.
[161] *Ibidem*, p. 20.
[162] *Ibidem*, p. 21.
[163] *Ibidem,* p. 25.
[164] *Ibidem,* p. 25.
[165] *Ibidem,* p. 27.
[166] *Ibidem,* p. 27.

dans le cadre de ce quatrième et dernier pilier que s'inscrit le projet d'espace européen des données de santé. Par là, elle vise à « *la mise à disposition de vastes réserves communes de données dans des secteurs (…) dans lesquels l'utilisation des données aura un impact systémique sur l'ensemble de l'écosystème, mais aussi sur les citoyens* »[167]. Concrètement, la Commission a identifié neuf domaines dans lesquels elle prévoit la création d'espaces européens des données :

- Les données relatives à l'industrie ;
- Les données relatives au pacte vert ;
- Les données relatives à la mobilité ;
- Les données relatives à la santé ;
- Les données financières ;
- Les données relatives à l'énergie ;
- Les données relatives à l'agriculture ;
- Les données pour l'administration publique
- Et les données relatives aux compétences[168].

Nous ne pouvons pas détailler chacun de ces espaces, mais leur énumération nous permet de réellement nous rendre compte de ce que l'espace européen des données de santé est un projet qui s'inscrit dans une approche globale de la promotion des échanges sécurisés de données au niveau européen. Cette approche est parfois qualifiée par la doctrine d'approche en « silos », c'est-à-dire une approche qui s'adapte à la nature de l'objet qu'elle entend réglementer. Cette approche en silos est caractéristique de l'action de l'Union, qui en a déjà fait la démonstration quand il s'agissait d'adapter la régulation des plateformes en ligne. La Commission a adopté différents instruments, contraignants ou non, en fonction du domaine à réguler : *fakenews,* discours haineux, atteintes aux droits de propriété intellectuelle…[169].

La réglementation de ces différents espaces de données se voudra tant sectorielle, avec des règles façonnées en fonction de la nature spécifique des données de chaque espace, que transsectorielle, ce qui aura pour but d'éviter une fragmentation du marché unique, conséquence

[167] *Ibidem,* p. 27.
[168] *Ibidem,* p. 29.
[169] Voy. parmi d'autres le « Code européen de bonnes pratiques contre la désinformation » co-signé par la Commission européenne et par Facebook, Google, Twitter et Modzilla en octobre 2018 ; le « Code de conduite visant à combattre les discours de haine illégaux en ligne », co-signé par la Commission européenne et par Facebook, Microsoft, Twitter et YouTube en mai 2016.

préjudiciable d'actions incohérentes d'un secteur à l'autre[170]. La régulation, précise la Commission, se fera également sous une approche qui « *favorise l'expérimentation, l'itération et la différenciation,* [plutôt que] *d'adopter des règles ex ante lourdes et trop détaillées* »[171].

Pour conclure, on constate donc que, si la Commission reconnait le retard qu'elle accuse en matière de circulation des données, elle ne reste pas pour autant inactive dans le domaine et a déjà mis en place une stratégie solide des données, ponctuée d'actions concrètes à implémenter au niveau européen, parmi lesquelles cet espace européen des données de santé.

[170] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM (2020) 66 final, 19 février 2020, p. 15.
[171] *Ibidem*, p. 15.

Partie III. Questions juridiques

Au terme de la description de la plateforme eHealth, de la plateforme healthdata.be, et du projet d'espace européen des données de santé, l'occasion se présente de confronter ces trois plateformes à leur légitimité. La sauvegarde des valeurs de l'État de droit requiert en effet de porter une attention de tous les moments sur les systèmes mis en place par l'autorité publique. Si des remises en question continuelles de celles-ci seraient nuisibles à leur efficacité, un examen détaillé de leur fonctionnement au regard des prescriptions légales ne peut leur être que bénéfique, car il renforcera, d'une façon ou d'une autre, leur légitimité aux yeux des citoyens.

Après avoir brièvement interrogé la légitimité de ces plateformes sous l'angle formel (Chapitre I), nous nous pencherons plus longuement sur leur légitimité fonctionnelle (Chapitre II), pour terminer par une mise en garde par rapport à certains risques qui subsistent malgré tout (Chapitre III).

Titre I. Légitimité formelle

Par « légitimité formelle », nous entendons voir d'abord les avis rendus par différentes institutions concernées sur les échanges de données médicales réalisés par ces plateformes.

Au sujet des échanges permis par la **plateforme eHealth**, on rappellera tout d'abord que celle-ci répond à la volonté du législateur fédéral, puisqu'elle a été instituée par la loi du 21 août 2008[172]. Au niveau de la première couche (*metahub*), si on détricote quelque peu le fonctionnement de la plateforme, on notera que quantité de ses éléments de fonctionnement ont été approuvés par des délibérations de la section santé du Comité sectoriel de la sécurité sociale et de la santé. Il ressortait effectivement des compétences de cet organisme de « *veiller au respect des dispositions fixées par ou en vertu de la loi visant à la protection de la vie privée à l'égard des traitements de données à caractère personnel relatives à la santé* »[173]. C'est à cette fin qu' « [il] *peut formuler toutes recommandations qu'*[il] *juge utiles et aider à la solution de*

[172] Loi du 21 août 2008 relative à l'institution et à l'organisation de la plateforme eHealth et portant diverses dispositions, *M.B.*, 13 octobre 2008.
[173] Délibération n° 12/047 du Comité de sécurité de l'information relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement, CSSSS/17/148, 19 juin 2012, point 6, p. 4.

tout problème ou de tout litige »[174]. Dans ce cadre-là, il a notamment rendu une délibération[175] approuvant la manière dont la plateforme eHealth recueille et enregistre le consentement du sujet des données de santé, et une délibération[176] autorisant la communication de données par la plateforme dans le cadre de différentes applications web comme « eHealthConsent », « Therapeutic Links Management », « Consent management » et « Exclusions », qui permettent respectivement de consentir à l'échange de données de santé par la plateforme eHealth, de gérer la liste des relations thérapeutiques que le patient entretient, de gérer ses différents consentements comme celui pour le don d'organes, et de fixer certaines exclusions personnelles de professionnels de la santé dans l'accès aux données du patient. On voit donc par là que le fonctionnement de la plateforme eHealth est soumis à un certain contrôle, qui permet que tous ses aspects fonctionnels soient revus et approuvés par un organe de contrôle indépendant. Un récent rapport, réalisé par une coopération UCLouvain-ULB-VUB et dirigé par Yves Coppieters, conclut d'ailleurs que « *la plateforme eHealth a de beaux jours devant elle* »[177], du fait qu'elle remplissait actuellement ses buts premiers, et continuait d'ouvrir l'éventail de ses bénéfices à d'autres horizons, en instiguant de nouveaux chantiers tels qu'« eBirth », « Consult-RN », « ORTHOpedic Prothesis Identification »… Au niveau de la deuxième couche (*hubs*), on observe également que le Réseau Santé Wallon, par exemple, a obtenu l'autorisation de l'Ordre national des Médecins[178], ainsi qu'une autorisation de l'APD[179], à l'époque « Commission de la protection de la vie privée ».

En ce qui concerne la **plateforme healthdata.be** de Sciensano, sa mise en place est prévue dans les missions de Sciensano par la loi qui porte la création de l'institution. Le §4 de l'article 4 de la loi dispose en effet que « *Sciensano assure le traitement, en ce compris la collecte, la validation, l'analyse, le rapportage et l'archivage, des données à caractère*

[174] 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, article 46, §2.
[175] Délibération n° 12/047 du Comité de sécurité de l'information relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement, CSSSS/17/148, 19 juin 2012, p. 7
[176] Délibération n° 12/081 du Comité de sécurité de l'information relative à la communication de données à caractère personnel à la plate-forme eHealth et par la plate-forme eHealth dans le cadre de l'application web « eHealthConsent », du service web « Therapeutic Links Management », du service web « Consent Management » et du service web « Exclusions », CSSSS/17/078, 18 septembre 2012, p. 14.
[177] D. DOUMONT *et al.*, *Vie privée et intégration des données de santé. Working paper n° 3*, Projet BeLHIS, AGORA AG/JJ/139, Bruxelles, 2010, p. 16.
[178] Conseil national de l'Ordre des médecins, autorisation approuvant le concept Réseau Santé Wallon, Bruxelles, 22 décembre 2009.
[179] Délibération n° 50/2009 de l'Autorité de protection des données, autorisant la FRATEM à utiliser le numéro du Registre national pour la gestion du Réseau Santé Wallon, Bruxelles, 15 juillet 2009.

personnel notamment relatives à la santé publique ou en un lien avec la santé et d'autres informations scientifiques relatives à la politique de santé, dans le respect des lois applicables en la matière. A cette fin, Sciensano réalise des analyses scientifiques quantitatives et qualitatives sur la base des informations traitées en vue de soutenir la politique de santé. Sciensano peut également mettre des données et des informations traitées à disposition, moyennant les autorisations des comités sectoriels compétents »[180]. Le Comité sectoriel a précisément rendu différentes délibérations, dont une en particulier[181] qui valide l'architecture de la plateforme healtdata.be.

Enfin, on pourrait penser que le **projet d'espace européen des données de santé**, en raison de son état encore embryonnaire, n'aurait pas encore eu l'occasion de bénéficier d'une éventuelle légitimité auprès d'institutions établies. Ce serait sous-estimer la vivacité du Contrôleur européen à la protection des données, institution créée en 2004 pour « *veiller à ce que les institutions et les organes de l'UE respectent le droit des citoyens à la protection de leur vie privée lors du traitement de données à caractère personnel* »[182]. L'organe a déjà rendu un avis préliminaire[183] le 17 novembre 2020 au sujet du projet d'espace européen des données de santé. Dans cet avis, le Contrôleur européen « *soutient fermement les objectifs de promotion de l'échange de données relatives à la santé et de stimulation de la recherche médicale* »[184]. En réalité, le propos est plus nuancé, car il va rappeler toute une série de points essentiels en matière de protection des données, dont la Commission devra tenir compte lors de la mise en place de l'espace européen des données de santé. On aura l'occasion de les relever dans le titre suivant. Mais d'un point de vue purement binaire, l'avis préliminaire du Contrôleur européen à propos du projet est positif.

En conclusion, on constate donc que les trois plateformes examinées, qu'elles soient en état de fonctionnement depuis longtemps, depuis peu de temps, ou encore à l'état de projet, bénéficient toutes les trois d'une solide légitimité institutionnelle, exprimée tant *ex ante* dans des avis ou délibérations, qu'*ex post* via des rapports d'analyse.

---

[180] Loi du 25 février 2018 portant création de Sciensano, *M.B.*, 21 mars 2018, art. 4, §4.
[181] Délibération n° 15/009 du Comité de sécurité de l'information relative à la méthode générique d'échange de données à caractère personnel pseudonymisées et non pseudonymisées relatives à la santé, dans le cadre de healthdata.be et healthstat.be, CSI/CSSS/20/102, 17 février 2015.
[182] « Contrôleur européen de la protection des données | Union européenne », https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_fr, consulté le 3 mai 2021.
[183] Avis préliminaire n° 8/2020 du Contrôleur européen de la protection des données sur l'espace européen des données de santé, Bruxelles, 17 novembre 2020.
[184] *Ibidem*, p. 3.

Titre II. Légitimité fonctionnelle

Ce chapitre vise à analyser la légitimité fonctionnelle de chacune des trois plateformes décrites dans la deuxième partie. Par « légitimité fonctionnelle », on entend confronter le fonctionnement actuel des plateformes au regard des prescriptions légales, principalement du RGPD. La portée de cette analyse ne nous permettant pas d'analyser tous les mécanismes des plateformes au regard de tous les éléments du RGPD, on verra successivement la place accordée au consentement (Chapitre 1), la mise en œuvre de certains droits dont le sujet jouit en vertu du RGPD (Chapitre 2), et enfin la manière dont elles garantissent la sécurité des données (Chapitre 3).

Chapitre I. Place du consentement

Section 1. Plateforme eHealth

Comme expliqué en partie I, le traitement, et donc *a fortiori* l'échange des données personnelles de santé, est en principe prohibé par l'article 9, §1er du RGPD, dû à leur qualité de « catégories particulières de données à caractère personnel ». Il n'est envisageable que s'il entre dans le cadre d'une des exceptions très strictes, énumérées au §2.

À la lecture du libellé de l'article 9, §2, h) du RGPD, la plateforme eHealth aurait-elle pu se passer du consentement du sujet des données, au motif que « *le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale* » ? Il nous semble devoir répondre de façon négative à la question. En effet, et on le lit bien dans ses objectifs décrits dans la seconde partie, la plateforme eHealth vise concrètement à « faciliter » la communication des données d'un professionnel de la santé à un autre, à « améliorer » la prise en charge médicale, à « diminuer » les charges pour le patient… Toutes ces finalités, aussi louables soient-elles, ne permettent pas de qualifier l'échange des données personnelles des patients de « *traitement* ***nécessaire*** *aux fins de diagnostics médicaux, de la prise en charge sanitaire, ou de la gestion des systèmes de soins de santé* ».

C'est fort probablement la raison pour laquelle la plateforme eHealth est retombée sur l'exception de l'article 9, §2, a) du RGPD, qui autorise le traitement des données de santé si « *la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques* ». Le consentement est donc requis par la plateforme, et elle le recueille selon les modalités que l'on a vues dans la deuxième partie. La manière de recueillir le consentement du patient avait été approuvée, rappelons-le, par la délibération n° 12/047 du Comité sectoriel.

Section 2. Plateforme healthdata.be et projet d'espace européen des données de santé

Le patient attentif pourra soulever la remarque selon laquelle, s'il a effectivement donné son consentement au partage de ses données via la plateforme eHealth aux fins d'une meilleure circulation de son dossier patient entre les différentes structures de soins dont il pourrait avoir besoin, il n'a pas pour autant consenti à l'envoi de ses données de santé à l'organisme Sciensano, pour lequel la plateforme healthdata.be réalise des objectifs qui sortent de ce champ.

Mais c'est précisément parce que les objectifs de la plateforme healthdata.be sont différents que celle-ci peut se passer du consentement des patients sujets des données qu'elle récolte. Elle peut en effet se baser sur l'exception de l'article 9, §2, j) qui permet l'échange des données de santé si leur traitement « *est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* »[185]. La plateforme healthdata.be, avec ses objectifs de statistiques (contribution à healthstat.be) et de recherche scientifique (fourniture des données aux centres de recherche) remplit la condition du traitement nécessaire aux fins mentionnées.

On peut toutefois soulever la présence de renforcements à cette exception, par les termes « *proportionné* », « *respecter l'essence du droit à la protection des données* », et « *prévoir des*

[185] Art. 9, §2, j) du Règlement (UE) 2016/679 (RGPD).

mesures appropriées et spécifiques ». Il nous semble que la plateforme healthdata.be satisfait à ces trois conditions. D'abord, la proportionnalité du traitement est rencontrée en ce que son processus, qui implique de requérir les données déjà référencées par la plateforme eHealth, ne rajoute pas de « poids » supplémentaire dans le chef du citoyen, au regard des bénéfices dont il jouit, certes indirectement, en tant qu'élément de la société, elle-même intéressée par la recherche scientifique. Ensuite, la collecte pour les fins de statistiques, au vu de la qualité de « globalisantes » de celles-ci, ne va pas à l'encontre de l'essence du droit à la protection des données. Enfin, des mesures spécifiques et appropriées sont mises en place : codage, anonymisation, agrégation des données… On aura l'occasion d'en reparler dans le chapitre III, en même temps que du contenu de l'article 89, §1, mentionné dans l'exception ici exploitée.

À noter également que le même raisonnement peut être tenu par analogie au projet d'espace européen des données de santé, puisque celui-ci correspond, à peu de choses près, à une adaptation au niveau européen de la plateforme healthdata.be.

Section 3. Conclusion sur la mise en œuvre de l'exigence de consentement

On peut donc constater que les trois plateformes, bien que soumises à des règles différentes en matière de consentement du sujet, peuvent toutes afficher une certaine légitimité fonctionnelle du fait qu'elles opèrent en accord avec les dispositions légales qui les concernent. Pris sous un autre angle, le constat peut aussi signifier que les outils légaux (principalement le RGPD) ont prévu les différentes possibilités de traitement des données médicales, en restreignant plus ou moins fortement la facilité d'y procéder, en ce qu'ils touchent de manière plus ou moins proche à la vie privée du sujet des données, qui pourra alors, ou non, opposer son droit au consentement.

Chapitre II. Mise en œuvre des principes et des droits du sujet

On l'a vu dans la première partie, le RGPD fixe certains principes relatifs au traitement des données, et confère, au sujet de ces données, une série de droits qu'il peut revendiquer face au responsable du traitement. Après avoir consacré tout un chapitre au droit au consentement, voyons ici comment les plateformes d'échange des données médicales mettent en œuvre certains de ces principes et droits. Pour des raisons pratiques, nous avons choisi de développer un des principes du traitement (Section 1) et un des droits du sujet (Section 2).

Section 1. Principe de limitation des finalités

Parmi ceux-ci, le principe de limitation des finalités (article 5, §1, b) du RGPD[186]) implique que le responsable du traitement ne collectera les données personnelles du sujet que pour des finalités « *déterminées, explicites et légitimes* », et ne les utilisera pas, par la suite, de façon incompatible avec ces finalités.

La plateforme eHealth nous semble respecter ce principe en ce que le prestataire de soins de santé, on l'a vu, ne peut accéder qu'aux données de santé « *pertinentes et non excessives au regard de la prise en charge de la santé de la personne concernée* »[187]. La prise en charge médicale est bien une finalité qui a été déterminée avec le patient de façon explicite et légitime dans son propre intérêt. De plus, l'exigence d'une relation thérapeutique de soins nous parait renforcer encore plus la mise en œuvre de ce principe, car elle permettra d'empêcher qu'un professionnel de soins de santé, qui aurait la qualification nécessaire pour accéder aux données, mais pas forcément les bons motifs, comme la prise en charge médicale du patient, ne fasse un usage des données incompatible avec la finalité d'une prise en charge médicale optimale.

La plateforme healthdata.be et le projet d'espace européen des données de santé semblent également respecter l'essence de cette disposition, puisque l'article 5, §1, b précise lui-même que « *le traitement ultérieur à des fins archivistiques dans l'intérêt public, **à des fins de recherche scientifique** ou historique **ou à des fins statistiques** n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales* ». Par l'entremise des finalités déterminées, explicites et légitimes de la plateforme eHealth, par

[186] Art. 5, §1er, b) du Règlement (UE) 2016/679 (RGPD).
[187] Règlement eHealth, p. 6.

laquelle les données de santé transitent, leur réemploi par nos deux plateformes d'agrégation de ces données affiche lui aussi une adéquation certaine avec le principe de finalité, car ce réemploi est abstraitement assimilé à une « finalité compatible » par le RGPD.

Section 2. Droit à la portabilité

En réalité, et d'un point de vue purement technico-légal, tous les échanges de données réalisés par ces trois plateformes d'échanges de données de santé des patients s'inscrivent dans la mise en œuvre du droit à la portabilité des données, dont ils bénéficient en vertu de l'article 20 du RGPD. Le texte de l'article mérite notre attention, tant il colle à la réalité concrète de ces systèmes :

« *1. Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque :*

a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b); et

b) le traitement est effectué à l'aide de procédés automatisés.

2. Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible. (…) » [188].

Si l'on applique la disposition à nos situations concrètes d'échanges de données médicales, on comprend bien toute la portée de l'article 20.

La plateforme eHealth, tout d'abord, échange les données des patients sur base de leur consentement, exigé sur base de la l'art. 9, §2, a), comme expliqué dans le chapitre précédent (*cf. supra*). Leur traitement est bel et bien automatisé. De plus, le fait que chaque prestataire, chaque hôpital qui accède à ces données peut le faire via cette plateforme d'échange, cela montre que la plateforme met également en œuvre le second paragraphe de la disposition, car,

[188] Art. 20 du Règlement (UE) 2016/679 (RGPD).

ce faisant, la plateforme eHealth est réellement le support qui permet que « les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre ».

Démontrer à quel point le droit à la portabilité des données personnelles épouse les formes de l'échange des données de santé est peut-être une bonne occasion pour nous de soulever également certaines faiblesses de l'article 20, qui pourraient en réalité limiter son applicabilité aux nécessités concrètes d'échange des données de santé. Dès lors que la Commission a relevé une certaine « *fragmentation dans la mise en oeuvre du droit à la portabilité des données de santé* »[189] dans sa stratégie pour les données de 2020, l'article 20 mérite en effet que l'on se penche sur sa formulation.

La disposition limite en réalité elle-même sa portée par sa formulation. D'une part, le troisième paragraphe de l'article 20[190] empêche l'application de ce droit aux missions d'intérêt public[191]. Cela posera problème dès lors qu'on considère que les plateformes healthdata.be et le futur espace européen des données de santé poursuivent ce type de mission. Ensuite, le Comité européen de la protection des données (CEPD), autre organe qui entre en jeu et veille, lui, à garantir une application cohérente du RGPD dans l'Union[192], a précisé que « *le droit à la portabilité des données concerne les données fournies sciemment et activement par la personne concernée ainsi que les données à caractère personnel générées par son activité* »[193]. Dans ce cadre, des données dérivées de l'évaluation de la santé d'un patient, comme le diagnostic médical, ne constitueraient donc pas des données « sciemment fournies par » le patient, et rendrait le droit à la portabilité inapplicable à ces données. Dans son avis préliminaire sur le projet d'espace européen des données de santé, le Contrôleur européen à la protection des données encourage pourtant la mise en œuvre du droit à la portabilité des données de santé[194]. Peut-être était-ce là l'occasion de proposer une réécriture de l'article 20 du RGPD. On pourrait donc rester quelque peu sur sa faim en lisant dans ses conclusions et recommandations que, à

[189] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM (2020) 66 final, 19 février 2020, p. 29.
[190] Art. 20, §3 du Règlement (UE) 2016/679 (RGPD).
[191] Avis préliminaire n° 8/2020 du Contrôleur européen de la protection des données sur l'espace européen des données de santé, Bruxelles, 17 novembre 2020, point 42, p. 15.
[192] « Who we are | European Data Protection Board », https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en, consulté le 4 mai 2021.
[193] Lignes directrices relatives au droit à la portabilité des données, Groupe de travail « Article 29 » sur la protection des données, telles que révisées et adoptées le 5 avril 2017, et approuvées par le Comité européen à la protection des données le 25 mai 2018, WP 242 rev.01, 13 décembre 2016.
[194] Avis préliminaire n° 8/2020 du Contrôleur européen de la protection des données sur l'espace européen des données de santé, Bruxelles, 17 novembre 2020, point 45, p. 16.

la place, l'institution invite indirectement les États membres à garantir eux-mêmes « *l'application du droit à la portabilité des données et l'élaboration, dans le cadre de l'espace européen des données de santé, des exigences techniques nécessaires permettant aux personnes concernées d'exercer effectivement ce droit* »[195]. Les États membres ne seront pas seuls, car la Commission prévoit elle aussi de « *prendre des mesures pour renforcer l'accès des citoyens aux données de santé et la portabilité de ces données* »[196].

Section 3. Conclusion sur la mise en œuvre des principes et des droits

En conclusion, pour le principe de finalité du traitement et pour le droit du sujet à la portabilité de ses données de santé, on constate que les trois plateformes suivent les prescrits légaux en la matière.

Plus fort encore, le droit à la portabilité est vraiment le concept au cœur du mécanisme de l'échange des données médicales, en ce qu'il permet d'assurer le droit du patient de pouvoir transporter facilement toutes ses données de santé avec lui auprès de n'importe quel prestataire de soins de santé. À cette nuance près que la rédaction originale de la disposition portant le droit à la portabilité pourrait poser des obstacles malencontreux à sa bonne applicabilité dans le cas d'espèce. Mais des mesures sont prévues, tant au niveau national qu'au niveau européen, pour garantir le succès du projet d'espace européen des données de santé dans ce domaine. Une occasion possible serait celle du « *Data Act* » prévu pour 2021[197].

Il est donc permis de conclure que les trois plateformes qui permettent la circulation des données de santé affichent une solide légitimité fonctionnelle, non seulement en ce qu'elles suivent les exigences légales en termes de protection des données personnelles, mais aussi en ce qu'elles apportent réellement leur pierre à l'édifice de la mise en œuvre continuelle des droits du sujet.

[195] *Ibidem*, point 59, p. 17.
[196] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM (2020) 66 final, 19 février 2020, p. 29.
[197] *Ibidem*, p. 21.

Chapitre III. Garanties de sécurité des données

Section 1. Anonymisation et pseudonymisation

L'article 32 du RGPD prévoit que le responsable du traitement des données personnelles doit mettre en œuvre différentes mesures, techniques et non techniques, pour garantir un niveau de sécurité adapté lors de ce traitement. Au premier rang de celles-ci figurent « *l'anonymisation et le chiffrement des données à caractère personnel* »[198].

Comme on l'a vu en partie I, la pseudonymisation des données est une mesure qui va « détacher » la donnée du sujet identifié, en lui attachant un autre identifiant, différent. Une pseudonymisation des données de santé implique que la base de données pseudonymisées ne contiendra que des données (données de santé) qui seront reliées à ce nouvel identifiant (« pseudonyme »), sans l'identifiant initial (le nom de la personne), tandis qu'une autre base de données contiendra, elle, les correspondances entre les deux identifiants (pseudonyme et nom de la personne), mais sans les données y relatives (informations sur la santé).

La **plateforme eHealth** a recours à ce procédé de pseudonymisation. Les banques de données des institutions (hôpitaux, médecins généralistes…) contiennent les données que sont le nom du patient, et ses données de santé. La banque-carrefour de la sécurité sociale contient dans ses données les identifiants que sont le nom du patient et son numéro d'inscription à la sécurité sociale (NISS). En utilisant le NISS pour isoler les données de santé entre elles, le *metahub* eHealth repère celles-ci dans les différents *hubs*, et cela sans qu'à un seul moment dans le processus la plateforme eHealth n'ait accès à la combinaison du nom du patient et de données de santé reliées à lui. Le NISS sert donc ici de pseudonyme. La plateforme eHealth remplit donc bien l'obligation de mettre en place des garanties de la sécurité du traitement.

L'article 89, §1er du même règlement[199] reprend cette exigence de garanties, en l'appliquant de façon explicite à l'exception de traitement à des fins de recherche scientifique ou à des fins statistiques qui, rappelons-le, permet au responsable du traitement de se passer du consentement du sujet des données personnelles. La **plateforme healthdata.be** met ce principe en œuvre, en le renforçant encore : elle reçoit les données anonymisées via la plateforme eHealth et leur fait ensuite subir un processus d'anonymisation.

[198] Art. 32 du Règlement (UE) 2016/679 (RGPD).
[199] Art. 89, §1er du Règlement (UE) 2016/679 (RGPD).

Également vu en partie I, l'anonymisation des données présente un niveau plus élevé de sécurité. En effet, si la pseudonymisation rend impossible l'identification de la personne sur base des données fournies en l'état, il reste toutefois possible de réidentifier la personne dès le moment où les différentes bases de données (BD1 : « nom + NISS », BD2 : « NISS + donnée de santé », BD3 : « nom + donnée de santé ») sont accessibles par le responsable du traitement, et où celui-ci décide de croiser celles-ci pour recouper les données entre elles. L'anonymisation, elle, est supposée rendre la personne totalement impossible à identifier sur base des données récoltées, même en procédant à de tels recoupements de données issues de différentes bases.

La plateforme healthdata.be va en réalité utiliser la plateforme eHealth comme « *trusted third party* » (« tiers de confiance »)[200] pour l'anonymisation des données qu'elle collecte. Concrètement, lors de l'envoi de données de santé à healthdata.be, la plateforme eHealth va coder ces données via le service « Batch_Codage »[201]. Cette méthode, qui opère, comme on l'a dit en partie II, au niveau de l'envoi par l'eHealthBox, est trop technique pour être détaillée dans un mémoire en droit. On retiendra simplement que Sciensano ne recevra que des données qui sont anonymisées par ce codage, de telle sorte qu'une personne derrière la plateforme, même si elle disposait d'une des bases de données initiales, ne pourrait pas recouper les données, car elle ne pourra pas relier la donnée obtenue après codage à l'identifiant détenu avant codage. De plus, lorsque Sciensano envoie les données stockées dans son *datawarehouse* aux bénéficiaires de ses services, ces derniers ne les reçoivent toujours que sous forme agrégées, donc de sorte à ce que seules des données « collectives » puissent apparaitre. Il semble donc que la plateforme healthdata.be respecte la garantie d'anonymisation, qui, quand elle est bien réalisée, rend impossible le fait d'identifier le sujet des données, ce qui lui permet de ne plus devoir recueillir son consentement.

Gageons qu'il en soit de même lors de la mise en place du **projet d'espace européen des données**. Dans tous les cas, la Commission est prévenue de cette nécessité par le Contrôleur européen à la protection des données, et reste également sous l'œil attentif du Comité européen à la protection des données, qui vérifiera l'adéquation de l'espace européen avec ces prescrits contenus dans le RGPD.

---

[200] « eHealth – Codage, anonymisation et trusted third party », https://www.ehealth.fgov.be/ehealthplatform/fr/codage-anonymisation-trusted-third-party, consulté le 4 mai 2021.

[201] Manuel de l'utilisateur de Batch codage, TTP eHealth, 23 juillet 2018, p. 1.

Section 2. Autres mesures

La disposition que nous venons de voir (article 32 du RGPD) ne mentionne pas uniquement la pseudonymisation comme garantie à mettre en place pour assurer la sécurité du traitement des données. Elle prévoit en effet que le responsable doit mettre en œuvre « *les mesures techniques et organisationnelles appropriées* »[202]. Voyons donc, outre la pseudonymisation et l'anonymisation qu'elles affichent, comment les trois plateformes protègent bien les échanges de données de santé.

La **plateforme eHealth** a pris une série de mesures techniques qui offrent des garanties de sécurité du traitement : outre son codage « Batch_TTP », elle a totalement sécurisé la eHealthBox via une identification eID/itsme® obligatoire[203] ou authentifie toute connexion au moyen de certificats eHealth[204], par exemple. De plus, tout accès à des données de santé est passible de contrôle car il est à chaque fois enregistré sur base des données de *logging*. Concrètement, toute demande sera enregistrée autour de quatre éléments : « qui » (la personne qui a accédé aux données), « quoi » (le sujet des données consultées), « quand » (le moment où s'est produit l'accès) et « comment » (l'application qui a permis l'accès aux données). Ce système (supporté par le module « *SecurityLogging* ») permet donc d' *« enregistrer tous les accès en lecture, écriture et suppression, qui auront force de preuve si plainte est déposée à cet égard* »[205]. Enfin, il est bon de soulever que tous les messages à destination des prestataires de soins sont cryptés avec un service de type « *end-to-end* »[206]. La plateforme eHealth a également pris des mesures non techniques (qualifiées d' « organisationnelles » dans le RGPD). Sur le plan de la sécurité de l'information, elle met en place tout un plan de sécurité de l'information, qui reprend, entre autres, « *la description des tâches, des responsabilités et des compétences au sein de l'organisation (…), la liste des responsabilités pour l'exécution concrète (…), les moyens de fonctionnement concrets (budget, ressources) à prévoir (sur base annuelle), l'état*

[202] Art. 32 du Règlement (UE) 2016/679 (RGPD).
[203] « eHealth – Boîte aux lettres électronique sécurisée », https://www.ehealth.fgov.be/ehealthplatform/fr/boite-aux-lettres-electronique-securisee, consulté le 4 mai 2021.
[204] « eHealth - Certificats eHealth », https://www.ehealth.fgov.be/ehealthplatform/fr/certificats-ehealth, consulté le 4 mai 2021.
[205] « eHealth – Gestion des loggins », https://www.ehealth.fgov.be/ehealthplatform/fr/gestion-des-loggings, consulté le 4 mai 2021.
[206] « eHealth – Système de cryptage end-to-end », https://www.ehealth.fgov.be/ehealthplatform/fr/systeme-de-cryptage-end-to-end, consulté le 4 mai 2021.

de la situation et/ou les actions à prendre »[207]. Sur le plan de la protection des données elle-même, la plateforme organise des formations pour les délégués à la protection des données (« *Data protection Officer, D.P.O.* ») et pour les conseillers en sécurité des entreprises qui ont recours aux services de la plateforme[208]. Elle a également adopté les normes minimales[209] élaborées par la Banque-carrefour de la sécurité sociale pour le secteur de la santé, basées sur la série ISO 27000[210], et à la base desquelles « *le délégué à la protection des données élabore la politique de sécurité de l'information* »[211].

La **plateforme healthdata.be** met en place, elle aussi, une série de mesures techniques pour garantir la sécurité. Avant tout, rappelons que, du fait qu'elle utilise les données transitées par la plateforme eHealth, elle bénéficie déjà d'un certain niveau de sécurité grâce à toutes les mesures mises en place par celle-ci. Ensuite, Sciensano affiche un système de gestion des utilisateurs en cascade, grâce auquel seul un nombre très limité d'utilisateurs ont accès aux données les plus sensibles[212]. Rappelons aussi, au titre des mesures techniques, que la plateforme crypte elle-même une seconde fois les données, et que ces dernières arrivent sous forme agrégée à l'utilisateur final. Là aussi, les données de *logging* sont enregistrées, rendant « *récupérable chaque utilisateur, accès, période d'accès, activité et résultat de cette activité* »[213]. C'est le logiciel InfoSphere Guardium produit par IBM qui permet d'accéder à ces données[214]. D'autres mesures, toujours plus techniques, renforcent encore la sécurité des données sur la plateforme. Au titre des mesures organisationnelles, précisons simplement que Sciensano a recruté un responsable sécurité et un professionnel des soins de santé, ainsi qu'un pool d'experts externes en « Small Cell Risk Assessment ». Leurs rôles sont comparables à ceux du responsable du plan de sécurité de l'information de la plateforme eHealth[215].

---

[207] « eHealth – Sécurité de l'information & Vie privée », https://www.ehealth.fgov.be/ehealthplatform/fr/service-securite-de-linformation-vie-privee, consulté le 4 mai 2021.
[208] *Ibidem*.
[209] Normes minimales de la Banque-carrefour de la sécurité sociale pour la sécurité de l'information et la vie privée dans le secteur de la santé, 7 mars 2017.
[210] « ISO 27001, la norme pour la sécurité de l'information », https://www.nbn.be/fr/iso27001, consulté le 4 mai 2021.
[211] « eHealth – Normes minimales », https://www.ehealth.fgov.be/ehealthplatform/fr/normes-minimales
[212] https://healthdata.sciensano.be/fr/protection-de-la-vie-priv%C3%A9e, consulté le 4 mai 2021.
[213] *Ibidem*.
[214] « IBM InfoSphere Guardium – IBM Documentation », https://www.ibm.com/docs/en/psfoa/1.1.0?topic=tasks-infosphere-guardium, consulté le 4 mai 2021.
[215] « Protection de la vie privée | healthdata.be », https://healthdata.sciensano.be/fr/protection-de-la-vie-priv%C3%A9e, consulté le 4 mai 2021.

Section 3. Conclusion sur la sécurité des données

En conclusion, on peut raisonnablement constater que les deux plateformes belges d'échange des données ont mis en place une série de mesures visant à protéger la sécurité des données personnelles. Au premier rang de celles-ci, beaucoup de procédés informatiques visant à pseudonymiser, anonymiser, coder, crypter les données, rendant celles-ci inutilisables en l'état à des fins autres que celles initialement autorisées. Dans les deux cas, même les accès prévus sont rigoureusement réglés, et en tout temps enregistrés pour un éventuel contrôle *a posteriori*. Il s'agit là de mesures techniques.

Mais elles ne sont pas les seules mesures prises pour protéger la sécurité des données. D'autres mesures, plus organisationnelles que techniques, ont également été mises en œuvre dans le même but. Entre plans de sécurité et délégués à la protection des données, on constate que ces mesures sont bien plus orientées vers les ressources humaines des deux structures. À noter d'ailleurs que l'engagement d'un DPO est maintenant une obligation pour ce type d'institutions en vertu de l'article 37, §1er, c) du RGPD[216], du fait de la quantité et de la qualité des données concernées par l'échange de données de santé.

On peut donc conclure que les deux plateformes réalisent une bonne mise en œuvre de l'article 32 du RGPD[217], qui exige la mise en place de telles mesures. À ce titre, elles présentent donc également une solide légitimité fonctionnelle.

L'espace européen des données de santé, parce qu'il n'est encore qu'à l'état de projet, ne bénéficie pas à ce stade de telles mesures de sécurité. Toutefois, en raison de sa place centrale dans le système de droit européen, nul doute que le futur instrument qui le mettra en place portera une attention particulière à cette exigence légale. Les différentes instances européennes de contrôle se sont en tout cas déjà déclarées prêtes à y veiller[218].

[216] Art. 37, §1er, c) du Règlement (UE) 2016/679 (RGPD).
[217] Art. 32 du Règlement (UE) 2016/679 (RGPD).
[218] Avis préliminaire n° 8/2020 du Contrôleur européen de la protection des données sur l'espace européen des données de santé, Bruxelles, 17 novembre 2020, point 46, p. 16.

Titre III. Perspectives et risques

La légitimité dont jouissent les plateformes actuelles d'échange de données médicales en Belgique découle donc principalement de leur compatibilité avec les exigences légales en matière de protection des données. Toutefois, cette caractéristique n'est pas chose assurée d'emblée pour toute situation de circulation de ces données, actuelles ou à venir. Le respect du droit à la vie privée et à la protection des données personnelles nécessite une attention de tous les jours. C'est à ce titre qu'il nous paraissait donc essentiel de consacrer les dernières pages de cette analyse aux perspectives et aux risques que ces plateformes pourraient aussi présenter.

Chapitre I. Les plateformes actuelles : 'Data against corona'

Il est difficile aujourd'hui de rédiger un mémoire qui touche à la santé sans évoquer l'impact de la crise sanitaire sur son sujet… L'eSanté a un rôle de première ligne à jouer dans la lutte contre l'épidémie et de nouvelles applications ont vu le jour en la matière. La Task Force « *Data & Technology against Corona* » a été mise en place pour coordonner les travaux[219].

Un représentant de l'Autorité belge de protection des données (ci-après, « APD ») fait partie de cette Task Force et veille au respect des recommandations formulée par l'autorité en matière d'applications de santé mobile[220]. Ces recommandations insistent sur trois points. D'abord, le traitement de données effectué par l'application doit être aussi limité que possible. S'il n'est pas nécessaire de traiter des données personnelles, il faut privilégier tant que possible l'anonymat de l'utilisateur. L'APD en profite d'ailleurs pour insister sur l'impossibilité totale de réidentifier le sujet, même en recoupant différentes données, pour pouvoir prétendre à une réelle anonymisation (*cf. supra*). Ensuite, elle recommande que soit expressément mentionnée la relation thérapeutique en cas d'utilisation d'une application dans ce cadre. Elle rappelle à ce titre aux professionnels de la santé le principe de finalité. Enfin, pour les cas qui ne rentrent ni dans le cadre du traitement de données anonymes, ni dans le cadre d'une relation thérapeutique, l'APD rappelle, dans un langage clair, tous les principes du RGPD auxquels le responsable du traitement doit se conformer pour l'utilisation de son application.

[219] « Le rôle de la Task Force 'Data & Techology against Corona' », https://www.ehealth.fgov.be/fr/esante/task-force-data-technology-against-corona/le-role-de-la-task-force-data-technology-against-corona, consulté le 5 mai 2021.
[220] « Applications de santé | Autorité de protection des données », https://www.autoriteprotectiondonnees.be/citoyen/themes/covid-19/applications-de-sante-, consulté le 5 mai 2021.

La plateforme eHealth nous informe également sur son site que le Comité de sécurité de l'information a défini une série de bonnes pratiques destinées aux plateformes de soins à distance. Il s'agit pour l'essentiel de conditions minimales (qui reprennent, entre autres, l'exigence du consentement du patient, d'un cryptage end-to-end, de méthodes d'authentification solides…) et de règles d'utilisation (incluant l'interdiction d'enregistrement d'une réunion vidéo de consultation, la présence et l'accessibilité des différents documents médicaux tels que les prescriptions électroniques ou les rapports de soins, sur l'application eSanté de la plateforme eHealth)[221].

La crise sanitaire a bousculé tous les secteurs, y compris celui des plateformes en ligne. Pour faire face à la crise, les autorités ont pris des mesures qui peuvent aboutir à faire planer au-dessus du citoyen une menace pour ses droits fondamentaux, y compris son droit à la vie privée. Les violations de celui-ci seront donc logiquement empêchées par l'autorité publique également, qui met en place différents organes (APD, Task Force, CSI…) chargés de veiller aux différents aspects de la vie privée dans le développement des solutions qu'elle propose.

Chapitre II. Une potentielle dérive : Projet de la Smals

Mentionner à ce stade le Comité de la sécurité de l'information nous fournit une occasion en or d'attirer l'attention du citoyen sur de potentielles dérives en matière d'échanges des données. Il nous faut garder un solide esprit critique envers ce Comité. En effet, l'institution est très souvent et violemment décriée dans la presse par les experts en protection des données. Ce chapitre vise à synthétiser les reproches que ces derniers adressent à la gestion des données par l'État belge, méthodiquement repris dans un article de presse rédigé avec finesse par M. Philippe Laloux, responsable du pôle Multimédias au quotidien Le Soir[222].

Le Comité de sécurité de l'information pose de sérieux problèmes d'indépendance et de légitimité. Une personne, du fait de sa présence à de multiples endroits de l'architecture informatique belge, concentre sur lui le feu des critiques : Frank Robben.

[221] « Bonnes pratiques en matière de plateformes pour les soins à distance », https://www.ehealth.fgov.be/fr/esante/task-force-data-technology-against-corona/bonnes-pratiques-en-matiere-de-plate-formes-pour-les-soins-a-distance-formulees-par-le-comite-de-securite-de-linformation, consulté le 5 mai 2021.

[222] P. LALOUX, « Le CSI, le club échangiste des gestionnaires de données », *Le Soir*, 10 février 2021.

À l'époque déjà directeur de la plateforme eHealth et de la Banque-carrefour de la sécurité sociale, Frank Robben est également celui qui a soutenu, via l'ancienne ministre de la santé Maggie De Block, le projet de loi qui visait à créer le Comité de sécurité de l'information, ci-après « CSI ». L'institution a été mise en place, contre les avis du Conseil d'État[223] et de l'APD[224] qui démolissaient ce projet, « *totalement hors-la-loi* ». Actuellement, Frank Robben assume encore beaucoup de fonctions, à savoir, entre autres : membre du Centre de connaissances de l'APD, gestionnaire général de la plateforme eHealth, membre du Comité général de coordination de la Banque-carrefour de la sécurité sociale, membre aviseur de la section Sécurité sociale et Santé de ce fameux Comité de la sécurité de l'information, membre du collège des directeurs de l'asbl « Egov », CEO de la Smals (l'ASBL informatique de l'État belge), etc… Seule une moitié des mandats publics, repris sur son propre site web[225], figure ici. On peut donc constater que l'informaticien est présent dans toutes les instances qui touchent de près ou de loin à la circulation des données personnelles des citoyens vers l'autorité publique.

Frank Robben est l'une des personnes qui a le plus œuvré à la mise en place d'une collecte des données décentralisée, « en silos » (comme le prévoit l'UE dans son projet de création d'espaces européens des données). On l'a vu, la décentralisation est le principe cardinal qui guidait l'autorité publique belge dans sa collecte de données. Toutes les données ne sont pas stockées en un seul endroit, mais dans différentes bases de données, en fonction de leur nature : les données de santé dans le réseau de la plateforme eHealth, les données sociales à la Banque-carrefour de la sécurité sociale, mais aussi les données fiscales, les données de justice, les données de mobilité… chacune dans leur institution respective. Là où le bât blesse, c'est que, chaque institution, chaque « réseau de données » était doté d'un « Comité sectoriel » (on a vu, en partie II, beaucoup de délibérations du Comité sectoriel sécurité sociale & santé), qui autorisait les dialogues entre différentes bases de données, parfois sensibles, alors que ces transferts de données n'étaient pas systématiquement légitimes. Heureusement, le RGPD est rapidement arrivé pour mettre fin à cette situation. La création de l'APD a mis fin à toutes ces

[223] Projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, 11 avril 2018, Avis de la section de législation du Conseil d'État n° 63.202/2, Doc. parl., Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 128

[224] Avis n° 34/2018 de l'Autorité de protection des données relatif à l'avant-projet de loi instituant le comité de sécurité de l'information […].

[225] « Public mandate overview – Frank Robben's personal website », https://www.frankrobben.be/about-me/public-mandate-overview/, consulté le 5 mai 2021.

autorisations d'échanges délivrées par les comités sectoriels. À partir de là, seule une loi pouvait autoriser une administration ou une institution à aller consulter les données dans une base de données d'une autre institution.

Mais c'est précisément à ce moment-là qu'a été votée la loi du 5 septembre 2018 instituant le Comité de sécurité de l'information. Le nouveau comité a récupéré la compétence de donner les autorisations pour les échanges de données. Ces dernières, qualifiées de « délibérations », sont signées par les deux sections du CSI : la plateforme eHealth, d'une part, et la Banque-carrefour de la Sécurité sociale, d'autre part. Or, ce sont précisément les deux organismes que Frank Robben dirige. Concrètement, il s'est donc légalement réservé le pouvoir de permettre lui-même les échanges de données (dont les données de santé), sans devoir passer à chaque fois par une loi. Ses délibérations, que la loi CSI a qualifiées de « normes »[226], échappent au contrôle du Conseil d'État, qui n'est compétent que pour contrôler les « actes administratifs »[227]. Elles échappent également au contrôle de l'APD, qui, selon la loi CSI, ne bénéficie que d'un « droit d'évocation »[228] contre ces délibérations. Dans une interview donnée au journal Le Soir et figurant toujours dans l'article de M. Laloux, Élise Degrave, chercheuse à l'UNamur et experte en protection des données personnelles, n'hésite pas à taper du poing en qualifiant la situation de « *tout à fait inconstitutionnelle* ».

Mais cela ne s'arrête pas là. La Smals, ASBL informatique de l'État (et accessoirement une autre institution pilotée par Frank Robben), travaille dans l'ombre depuis maintenant trois ans sur un projet nommé « *Putting data at the center* », ci-après « PDC ». Le projet vise à développer « *un immense carrefour où se croisent toutes les bases de données ultra-sensibles, traditionnellement décentralisées et inviolables* »[229]. Ce croisement des données à grande échelle permettrait évidemment des possibilités de réutilisations énormes. Or, c'est précisément le but avoué du projet : avoir une « *vision globale sur les citoyens et les entreprises* »[230]. D'ailleurs, plusieurs entreprises privées se seraient déjà présentées comme « clients potentiels ». Inutile de préciser les conséquences désastreuses qui surviendraient si des

[226] 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, art. 46, §1er, remplacé par la loi du 5 septembre 2018, *M.B.*, 10 septembre 2018.
[227] Lois coordonnées du 12 janvier 1973 sur le Conseil d'État, *M.B.*, 21 mars 1973, art. 14.
[228] Loi du 15 janvier 1990 précitée, *M.B.*, 22 février 1990, art. 46, §2, remplacé par la loi du 5 septembre 2018, *M.B.*, 10 septembre 2018.
[229] P. LALOUX, « Vie privée : un projet sans contrôle de l'État pour « profiler » les Belges », *Le Soir*, 10 mars 2021.
[230] *Ibidem.*

institutions déjà aussi puissantes, telles que les banques ou les assurances, entraient en possession des données sensibles des citoyens. Le risque de profilage du citoyen approche.

L'état de projet de PDC pourrait rassurer, mais le produit en serait déjà à sa 21e étape de fabrication, mobilisant six informaticiens de la Smals, pour un budget d'un à deux millions d'euros. Le « projet » est donc en passe d'aboutir. La Smals, qui ne bénéficie d'aucun mandat législatif, ministériel ou administratif, développe donc un projet dangereux, sans cadre légal. Impossible à contrôler, le projet « *Putting data at the center* » semble donc échapper au droit en vigueur. Or, il entre précisément en conflit avec ce droit en vigueur. En effet, à nouveau grâce aux propos d'Élise Degrave, on peut confirmer cette idée selon laquelle le RGPD s'en verrait gravement violé : « [le but du projet PDC d'offrir une vision globale sur les citoyens et les entreprises] *n'est pas une finalité valable* »[231], elle doit être autorisée par une loi. De plus, il apparait clairement qu'il méconnaitrait le principe de proportionnalité, qui veut que le responsable du traitement n'accède qu'aux données nécessaires et auxquelles l'accès est autorisé par la loi. L'on pourrait encore parler longuement de ce projet macabre, à propos duquel Frank Robben a d'ailleurs déclaré « *ne pas être au courant* » (propos repris à la toute fin de l'article du Soir), mais l'essentiel dans le cadre de cette analyse est de réaliser les trois constats suivants. Tout d'abord, l'architecture institutionnelle de la circulation des données vers le gouvernement pose, en Belgique, de sérieux problèmes d'indépendance, incarnés par la personne de Frank Robben, présent dans littéralement chacune des institutions concernées. Or, si les instituions de contrôle des plateformes d'échange des données venaient à perdre la confiance du citoyen, c'est tout le mécanisme de la circulation des données (de santé, entre autres), avec ses bénéfices par la même occasion, qui souffrira en y perdant sa légitimité. Ensuite, le citoyen doit rester alerte face aux agissements de l'autorité publique vis-à-vis de ses données les plus sensibles. Avec une architecture interne mal ficelée, ce genre de projet peut tout à fait se développer à son insu. La presse continue, heureusement, à jouer à cet égard son rôle de « chien de garde de la démocratie ». Enfin, il y a lieu de s'interroger sur la place du droit dans les perspectives d'échange des données. Alors que la loi est censée structurer ce genre de systèmes, il semble que certaines initiatives parviennent à se développer « en dehors du droit », au mépris total des règles les plus importantes, sans possibilité de contrôle législatif. Le politique a là clairement une place à (re)prendre, car le débat démocratique est actuellement le seul moyen de ne pas basculer dans une technocratie.

[231] *Ibidem.*

Chapitre III. Vie privée de l'enfant.

Pour terminer, on peut voir à quel point le sujet de la vie privée numérique, et surtout celui des données relatives à la santé, est un sujet brûlant, qui touche tout citoyen, et cela dès son plus jeune âge.

À titre d'illustration, on mentionnera l'exemple on-ne-peut-plus récent de la déclaration du Comité des Ministres du conseil de l'Europe du 29 avril 2021, par laquelle celui-ci vise à attirer l'attention sur la nécessité de veiller à la protection du droit au respect de la vie privée des enfants dans l'environnement numérique.

Rappelant d'abord que « *dans toutes les actions relatives à l'environnement numérique qui concernent les enfants, l'intérêt supérieur de l'enfant doit être une considération primordiale, en plus d'assurer* [le droit à la vie privée de l'enfant] »[232], il met en garde contre les risques humains pour les enfants qui peuvent découler de leur traçabilité dans l'environnement numérique : discrimination, harcèlement, intimidation… ainsi qu'aux risques numériques : prise de décision automatisée, profilage…[233].

Pour ce faire, il appelle donc à mettre en place « *des mesures de sécurité et de protection renforcées en ce qui concerne l'utilisation de la technologie et le traitement des données (…) relatives à la santé des enfants (…), afin de minimiser les effets négatifs potentiels, y compris l'identification publique d'un enfant comme porteur de la covid-19* »[234].

Si le propos peut sembler un peu décalé du cadre général de cette analyse, il y a pourtant toute sa place. En effet, dans la conception et la régulation des plateformes d'échange des données, il doit y avoir une attention constante non seulement au respect du droit à la vie privée de tout citoyen, mais encore plus à celui des enfants, qui sont les potentielles victimes les plus fragiles et les plus dénuées de recours face aux réelles conséquences d'un partage incontrôlé de leurs données de santé, permis par l'environnement numérique omniprésent.

[232] Déclaration du Comité des Ministres du Conseil de l'Europe relative à la protection du droit au respect de la vie privée des enfants dans l'environnement numérique, Decl(28/04/2021), 28 avril 2021, p. 1.
[233] *Ibidem*, p. 2.
[234] *Ibidem*, p. 3.

Conclusion

L'échange des données relatives à la santé du citoyen est un sujet qui, on le voit, soulève une foule de questions. Au regard des bénéfices qu'il réalise au quotidien, tant au niveau individuel (meilleure prise en charge médicale) qu'au niveau collectif (recherche scientifique plus performante), il est nécessaire que ces données de grande valeur circulent au mieux, et ce, à tous les niveaux : régional, national, et européen.

L'État belge, conscient de ces enjeux, a déjà pris le pas en fournissant deux plateformes d'échange des données de santé qui réalisent les bénéfices attendus. La plateforme eHealth permet un accès aux données de santé, tant par le patient sujet des données que par le professionnel de la santé qui a un intérêt légitime à y accéder. La plateforme healthdata.be de Sciensano fournit, quant à elle, ce double service de collecte des données de santé et de fourniture de celles-ci sous forme agrégée aux organismes de recherche scientifique et de politiques publiques.

L'Union européenne n'est pas en reste dans la promotion des échanges de données de santé. Reconnaissant pleinement la haute valeur intrinsèque des données, la Commission a prévu dans sa stratégie globale pour les données la création, parmi d'autres, d'un espace européen des données de santé. Celui-ci sera l'une des nombreuses pièces d'un espace européen des données, un « marché unique des données », ce qui est logique, tant les actions concrètes prévues par la Commission visent en réalité à instaurer une sorte de cinquième liberté fondamentale au sein du marché intérieur : la libre circulation des données.

Toutefois, si le citoyen a tout intérêt à gagner dans une bonne circulation des données de santé, il doit également être conscient des risques que celle-ci implique par rapport à son droit à la vie privée et à la protection de ses données personnelles.

Les différents instruments légaux présentés en première partie ont tous pour objectif de protéger ces deux droits fondamentaux. Après avoir détaillé leur fonctionnement en seconde partie, on a pu constater, lors de la troisième partie, à visée plus critique, que les trois plateformes d'échanges des données de santé bénéficiaient d'une solide légitimité, tant vis-à-vis des autres institutions du paysage public belge et européen, qu'au regard de leur

fonctionnement interne, qui respecte bien les exigences posées par le Règlement général relatif à la protection des données à caractère personnel.

Cependant, cette affirmation se doit d'être légèrement nuancée au vu des observations effectuées en fin de troisième partie. Certains doutes émis vis-à-vis de l'organisation structurelle du système de gouvernance des données en Belgique peuvent être de nature à remettre en cause cette légitimité. De plus, cette prise de recul a également été l'occasion de formuler une certaine mise en garde à l'attention du citoyen. S'il bénéficie bel et bien de plateformes solides et sécurisées d'échange des données de santé, ce n'est pas pour autant qu'il doit considérer ce respect de sa vie privée comme acquis. L'apparence de sécurité fournie par la décentralisation des données pourrait facilement être remplacée par un profilage rigoureux, invasif, mais surtout illégal, du comportement du citoyen.

Si la presse est bien le chien de garde, c'est le droit qui reste le maître. Le législateur ne doit pas oublier son rôle de garant de la démocratie, ni la place du droit au centre de toutes les possibilités soulevées par le progrès technologique. En démocratie, le droit encadre les procédés techniques mis en œuvre au service du citoyen. Quand c'est la technique qui adapte le droit pour contrôler le citoyen, on a basculé dans la technocratie.

Bibliographie

Législation

Législation belge

Normes

- Constit., art. 32.
- Lois coordonnées du 12 janvier 1973 sur le Conseil d'État, *M.B.*, 21 mars 1973.
- 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.
- Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.
- Loi du 11 avril 1994 relative à la publicité de l'administration, *M.B.*, 30 juin 1994.
- Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 26 septembre 2002.
- Loi du 21 août 2008 relative à l'institution et à l'organisation de la plateforme eHealth et portant diverses dispositions, *M.B.*, 13 octobre 2008.
- Loi du 4 mai 2016 relative à la réutilisation des informations du secteur public, *M.B.*, 3 juin 2016.
- Loi du 25 février 2018 portant création de Sciensano, *M.B.*, 21 mars 2018.
- Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *M.B.*, 10 septembre 2018.
- Protocole d'accord du 26 mars 2018 conclu entre le Gouvernement fédéral et les Autorités visées aux articles 128, 130, 135 et 138 de la Constitution, décrivant la collaboration entre les parties signataires en vue de l'utilisation de l'instrument BelRAI, *M.B.,* 4 juin 2018.

Travaux préparatoires

- Projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, 11 avril 2018, Avis de la section de législation du Conseil d'État n° 63.202/2, Doc. parl., Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 128

Législation de l'Union européenne

Règlements

- Règlement (UE) 2016/679 (RGPD) du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016.
- Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *J.O.U.E.*, L 303, 28 novembre 2018.

Directives

- Directive 65/46/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, *J.O.U.E.*, L 281, 23 novembre 1995.
- Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *J.O.U.E.*, L 345, 31 décembre 2003.
- Directive (UE) 2019/1024 du Parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, *J.O.U.E.*, L 172, 26 juin 2019.

Communications

- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Créer une économie européenne fondée sur les données », COM (2017) 9 final, 10 janvier 2017.
- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Permettre la transformation numérique des services de santé et de soins dans le marché unique numérique ; donner aux citoyens les moyens d'agir et construire une société plus saine », COM (2018) 233 final, 25 avril 2018.
- Communication de la Commission au Parlement européen et au Conseil, « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, COM (2019) 250 final, 29 mai 2019.
- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Une stratégie européenne pour les données », COM (2020) 66 final, 19 février 2020.
- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Façonner l'avenir numérique de l'Europe », COM (2020) 67 final, 19 février 2020, p. 13.

- Communication de la Commission portant proposition de règlement du Parlement européen et du Conseil sur la gouvernance des données, COM (2020) 767 final, 25 novembre 2020.

Travaux préparatoires

- Avis préliminaire n° 8/2020 du Contrôleur européen de la protection des données sur l'espace européen des données de santé, Bruxelles, 17 novembre 2020.
- Lignes directrices relatives au droit à la portabilité des données, Groupe de travail « Article 29 » sur la protection des données, telles que révisées et adoptées le 5 avril 2017, et approuvées par le Comité européen à la protection des données le 25 mai 2018, WP 242 rev.01, 13 décembre 2016.

Législation internationale

Normes

- Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, *err.* 29 juin 1961.
- Pacte international relatif aux droits civils et politiques, fait à New York le 19 décembre 1966, approuvé par la loi du 15 mai 1981, *M.B.*, 6 juillet 1983.
- Charte des droits fondamentaux de l'Union européenne, adoptée à Nice le 7 décembre 2000.

Autres actes

- Déclaration du Comité des Ministres du Conseil de l'Europe relative à la protection du droit au respect de la vie privée des enfants dans l'environnement numérique, Decl(28/04/2021), 28 avril 2021.
- *Guide sur l'article 8 de la Convention européenne des droits de l'homme*, Conseil de l'Europe, 31 août 2020.

Jurisprudence

Jurisprudence de la Cour constitutionnelle belge

- C.C., 18 octobre 2006, n°151/2006.

Jurisprudence de la Cour de Justice de l'Union européenne

- CJCE, arrêt *Österreichischer Rundfunk*, 20 mai 2003, aff. jtes C-465/00, C-138/01 et C-139/01, EU:C:2003:294.

❖ CJCE, arrêt *Lindqvist*, 6 novembre 2003, C-101/01, EU:C:2003:596.

Jurisprudence de la Cour européenne des droits de l'homme

❖ Cour eur. D.H., arrêt *Niemitz c. Allemagne*, 16 décembre 1992.

❖ Cour eur. D.H., arrêt *Pretty c. Royaume-Uni*, 29 avril 2002.

❖ Cour eur. D.H., arrêt *Peck c. Royaume-Uni*, 28 janvier 2003.

❖ Cour eur. D.H., arrêt *Leander c. Suède*, 26 mars 1987.

❖ Cour eur. D.H. (gde ch.), arrêt *Amann c. Suisse*, 16 février 2000.

Doctrine

❖ DE TERWANGNE, C., « Présentation générale du R.G.P.D. et des lois belges relatives à la protection des données », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle,* C. De Terwangne, E. Degrave, F. Henry, H. Jacquemin, T. Léonard, P. Limbrée, S. Parsa, I. Verhelst, Limal, Anthemis, 2020, p. 7 à 58.

❖ DE VISSCHER F., *et al.,* « Rights in data », *Ing.-Cons.,* 2020/2, Bruxelles, Larcier, 2020, p. 360 à 395.

❖ DEGRAVE, E., « Le R.G.P.D., les lois belges et le secteur public. Les traitements de données dans l'administration en réseaux et l'Autorité de protection des données », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, C. De Terwangne, E. Degrave, F. Henry, H. Jacquemin, T. Léonard, P. Limbrée, S. Parsa, I. Verhelst, Limal, Anthemis, 2020, p. 281 à 318.

❖ DELFORGE, A., « L'accès et la réutilisation des données du secteur public : entre ouverture et protection des données à caractère personnel », *B.S.J.*, n° 621 (Janvier 2019-2), 2019, p. 14.

❖ DOUMONT, D., COLS, F., D'HOORE, W., COPPIETERS, Y., DEBOOSERE, P., INGENBLEEK, A., LAMMENS, L., LEVÊQUE, A., *Vie privée et intégration des données de santé. Working paper n° 3*, Projet BeLHIS, AGORA AG/JJ/139, Bruxelles, 2010, p. 16.

❖ DUMONT, H., et HACHEZ, I., « Les obligations positives déduites du droit international des droits de l'Homme : dans quelles limites ? », *Les droits de l'Homme, bouclier ou épée du droit pénal ? ¸* Y. Cartuyvels, H. Dumont, F. Ost, M. Van De Kerckhove et S. Van Drooghenbroeck (dir.), Bruxelles, Bruylant, 2007, p. 45 à 73.

❖ ERGEC, R., « Chapitre 5. – Droits concernant la vie privée et la vie familiale », *Convention européenne des droits de l'homme*, J. Velu, R. Ergec (dir.), 2e édition, Bruxelles, Bruylant, 2014, p. 645 à 710.

- HENROTTE, J.-F., « De la distinction entre l'anonymisation et la pseudonymisation », *J.L.M.B.* 2020, n° 29, p. 1361 à 1363.
- HOEBEKE, S., et MOUFFE, B., *Droit de la presse. Presse écrite, presse audiovisuelle et presse électronique,* Limal, Anthemis, 2012, p. 474
- LEMMENS, K., « Le droit au respect de la vie privée et de la personnalité », *Les droits constitutionnels en Belgique*, M. Verdussen et N. Bonbled (dir.), Bruxelles, Bruylant, 2011, p. 901 à 931.
- PICOD, F., RIZCALLAH, C. et VAN DROOGHENBROECK, S., « Annexe - La Charte des droits fondamentaux et ses explications publiées le 14 décembre 2007 », *Charte des droits fondamentaux de l'Union européenne*, Bruxelles, Bruylant, 2019, p. 1383 à 1430.
- POULLET, Y., *La vie privée à l'heure de la société du numérique*, 1e édition, Bruxelles, Larcier, 2019, p. 67.
- POULLET, Y., « Le numérique et le droit à la rencontre des personnes âgées », *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, M.-C. Piatti et M. Guillermin (dir.), Paris, Editions des archives contemporaines, 2020, p. 85 à 109.
- STROWEL, A. et SOMAINI, L., « The Regulation of Non-Personal Data in the EU and the 2020 Data Strategy », *Propriété intellectuelle à l'ère du Big Data et de la Blockchain*, J. DE WERRA (dir.), Zürich, Schulthess, 2020, p. 29 à 58.
- TINIÈRE, R., « L'apport de la Charte des droits fondamentaux à la protection des données personnelles dans l'Union européenne », *Rev. Aff. Eur.*, 2018, p. 29 à 34.
- VILLANI, C., *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, 8 mars 2018.
- VON DER LEYEN, U., *Une Union plus ambitieuse. Mon programme pour l'Europe - Orientations politiques pour la prochaine Commission européenne 2019-2024*, 16 juillet 2019.
- X., « Dispositifs médicaux implantables et dispositifs médicaux de classe III », *B.I.-I.N.A.M.I.*, 2015/4, p. 74.

Articles de presse

- A. RAJAN, « Data is not the new oil », Réponse à *The Economist*, BBC News, 9 octobre 2017, http://www.bbc.com/news/entertainment-art-41559076, consulté le 21 avril 2021.
- P. LALOUX, « Le CSI, le club échangiste des gestionnaires de données », *Le Soir*, 10 février 2021.
- P. LALOUX, « Vie privée : un projet sans contrôle de l'État pour « profiler » les Belges », *Le Soir*, 10 mars 2021.

Divers

- E. CAMBERLIN, T. DEFOUR, Synthèse : « RGPD : Conseils aux professionnels de la santé », p. 2 https://www.dentiste.be/DocumentFromDatabase.aspx?id=205.

- Avis n° 34/2018 de l'Autorité de protection des données relatif à l'avant-projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, 11 avril 2018.

- Règlement du partage de données de santé entre les systèmes de santé connectés via le répertoire de références de la plate-forme eHealth, approuvé par la délibération n° 14/016 du 18 février 2014 du Comité de sécurité de l'information.

- Délibération n° 50/2009 de l'Autorité de protection des données, autorisant la FRATEM à utiliser le numéro du Registre national pour la gestion du Réseau Santé Wallon, Bruxelles, 15 juillet 2009.

- Délibération n° 11/046 du Comité de sécurité de l'information relative à la note concernant le consentement éclairé dans le projet des hubs et du metahub, CSSS/14/080, 17 mai 2011.

- Délibération n° 11/088 du Comité de sécurité de l'information relative à la note relative aux preuves électroniques d'une relation thérapeutique et d'une relation de soins, CSSSS/11/134, 18 octobre 2011.

- Délibération n° 12/047 du Comité de sécurité de l'information relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement, CSSSS/17/148, 19 juin 2012.

- Délibération n°14/016 du Comité de sécurité de l'information portant sur le règlement du partage de données de santé entre les systèmes de santé connectés via le répertoire de références de la plateforme eHealth, CSI/CSSS/20/442, 18 février 2014.

- Délibération n° 15/009 du Comité de sécurité de l'information relative à la méthode générique d'échange de données à caractère personnel pseudonymisées et non pseudonymisées relatives à la santé, dans le cadre de healthdata.be et healthstat.be, CSI/CSSS/20/102, 17 février 2015.

- Normes minimales de la Banque-carrefour de la sécurité sociale pour la sécurité de l'information et la vie privée dans le secteur de la santé, 7 mars 2017.

- Manuel de l'utilisateur de Batch codage, TTP eHealth, 23 juillet 2018.

Sites internet

- https://www.23andme.com
- http://www.bbc.com
- https://www.ehealth.fgov.be
- https://www.reseausantewallon.be
- https://www.sciensano.be
- https://www.absym-bvas.be
- https://www.support.healthdata.be
- https://www.healthdata.sciensano.be
- https://www.ec.europa.eu
- https://www.europa.eu
- https://www.edpb.europa.eu
- https://www.nbn.be
- https://www.ibm.com
- https://www.autoriteprotectiondonnees.be
- https://www.frankrobben.be

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/drt**