BIG DATA & PROTECTION DES DONNÉES DANS LE DOMAINE DE LA SANTÉ

Sébastien Fanti

Avocat et Notaire, Préposé à la protection des données et à la transparence du Canton du Valais, Sion

sebastien.fanti@sebastienfanti.ch

Le soussigné précise n'être lié ni contractuellement, ni économiquement à aucun acteur du Big Data, ni à aucun acteur dans le domaine du e-Health, respectivement du dossier patient. Les opinions émises le sont donc libres de toute contrainte ou influence.

Sommaire

1 INTRODUCTION

Lorsque sont évoquées les données médicales, chacun appréhende de manière personnelle les risques qui résultent de leur traitement. D'aucuns considèrent que leur perte ou leur vol sont le danger principal, alors que d'autres y voient le risque qu'un jour leur assureur soit capable de définir la prime en fonction d'un suivi quasi en temps réel de l'état de santé de la naissance à la mort. Mais il y a plus. Ces données, dans un monde où l'accès aux soins se révèle toujours plus onéreux, attisent les convoitises des cyberdélinquants en tous genres. L'usurpation d'identité médicale est l'une des composantes de la palette d'actes illicites toujours plus nombreux. Contrairement à l'usurpation d'identité économique qui peut engendrer jusqu'à la ruine, l'usurpation d'identité médicale peut vous coûter la vie. Qu'est-ce que l'usurpation d'identité médicale ? Selon le World Privacy Forum, un organisme à but non lucratif[1], il y a usurpation d'identité médicale « Lorsqu'une personne s'approprie le nom et d'autres informations pertinentes au profil médical d'un

1 Non profit, non-partisan public interest research group : <www.worldprivacyforum.org>.

patient, à son insu dans le but d'obtenir des soins médicaux ou des médicaments, ou lorsque cette personne utilise ces informations à des fins lucratives »[2]. L'usurpateur d'information médicale peut aussi utiliser des informations de tiers notamment pour obtenir des soins médicaux, des produits et médicaments nécessitant une ordonnance ou encore formuler des réclamations médicales frauduleuses. À cela s'ajoute bien évidemment l'aspect économique, avec la possibilité de vendre ces données au plus offrant pour un prix de l'ordre de 50 dollars par dossier médical[3] ! Peu connu, pour ne pas dire ignoré du grand public et des professionnels de santé, ce phénomène se développe et évolue de manière significative aux États-Unis. Les cas d'usurpation médicale recensés sont passés de 500'000 en 2006 à 1'500'000 en 2012, soit une augmentation de plus de 200% selon une étude réalisée par le World Privacy Forum en 2006[4] et les informations récoltées ultérieurement. Une carte interactive par ville américaine a même été réalisée pour que chacun puisse appréhender le risque géographiquement[5] ! Le Département de la justice de Californie a même émis en octobre 2013 des recommandations très précises pour éviter une prolifération de ces comportements criminels[6.] Quant au gouvernement fédéral, il a mis en service par l'intermédiaire de la Federal Trade Commission (FTC[7]) un site dédié comportant un outil de récu-

2 <https://www.worldprivacyforum.org/category/med-id-theft/>.

3 Ce prix a été communiqué au soussigné par un White Hat Hacker, soi un pirate informatique éthique qui réalise des tests d'intrusion, l'un des meilleurs mondiaux, puisque classés régulièrement dans les trois premiers du Defcon de Las Vegas (www.defcon.org), considéré comme le championnat du monde. Il s'agit du prix pratiqué dans le Dark Web, soit le web invisible utilisé par les pirates pour vendre illégalement des biens de consommation, des identités, des identifiants, des cartes de crédit, etc.

4 <https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/>.

5 <https://www.worldprivacyforum.org/2011/08/medicalidentitytheft-map/>.

6 Kamala D. Harris, Attorney General, California Department of JusticeMedical Identity Theft, Recommandations for the Age of Electronic Medical Records, octobre 2003, accessible à cette adresse :
<https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf>.

7 Il s'agit d'une agence indépendante du Gouvernement des États-Unis dont la mission principale est l'application du droit de la consommation et le contrôle des pratiques commerciales

pération online d'identité numérique[8], ce qui démontre l'ampleur actuelle de ce phénomène.

Vous m'objecterez certainement que ce pays, à l'inverse du nôtre, ne connaissait pas encore de régime d'assurance maladie aussi développé. Certes. Toutefois aujourd'hui en Suisse, il peut être constaté une difficulté croissante au règlement des primes d'assurance-maladie. Le risque est donc bien réel, même s'il est certainement moins saillant à ce jour.

Ainsi, les dangers liés au traitement des données médicales doivent-ils être considérés comme protéiformes, évolutifs et parfois létaux. La multiplication des données va provoquer une aggravation exponentielle du risque qu'il conviendra de juguler, ce qui ne sera pas aisé. L'appréhension de ce risque par des autorités distinctes (Ministère public, Préposé fédéral à la protection des données et Préposés cantonaux) complique également la tâche de ceux qui tendent par leurs actions à le rendre infinitésimal, ainsi que nous le verrons ci-après.

1.1 Définition du Big Data (« mégadonnées » ou « données massives »)

La notion de « Big Data » se réfère à une grande quantité de données provenant de sources diverses et qui sont saisies et enregistrées grâce à des systèmes de traitement à très haut débit, en vue de permettre leur exploitation et leur analyse sans but prédéterminé et sans limites de temps[9]. Comme le

anticoncurrentielles telles que les monopoles déloyaux. Elle s'est forgée une solide réputation de régulateur dans le domaine des nouvelles technologies et ses avis sont très respectés ; cf. <https://www.ftc.gov>.

8 <https://www.identitytheft.gov>.

9 Il s'agit de la définition du Préposé fédéral à la protection des données et à la transparence disponible sur son site Internet : <http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=fr>.

relève Michel Jaccard[10], appréhender ce concept n'est pas aisé. De façon générale, la notion recouvre un ensemble de technologies et d'approches qui ont pour but de s'appuyer sur des masses gigantesques de données pour en extraire des caractéristiques précises et fournir des outils de comparaison, de diagnostic, de pronostic et d'aide à la décision[11]. Rolf H. Weber[12] se réfère quant à lui à la définition suivante issue de Bitkom (Digital Verband Deutschland)[13] : « Einsatz grosser Datenmengen aus vielfältigen Quellen mit einer hohen Verarbeitungsgeschwindigkeit zur Erzeugung wirtschafltichen Nutzens ». La notion retenue influe évidemment sur les règles juridiques applicables de sorte qu'elle est importante. Deux éléments dans le cadre de la définition retenue par le soussigné sont, dans ce contexte à mettre en exergue, soit l'absence de but prédéterminé et le fait que ces données n'ont, intrinsèquement, aucune limitation temporelle sans intervention tierce.

Les caractéristiques du Big Data font l'objet d'une abréviation : 4V[14], soit :

Volume : les quantités de données traitées se comptent désormais en téraoctets, voire en pétaoctets.

Vélocité : les données doivent pouvoir être traitées à grande vitesse et immédiatement dès leur collecte, car leur valeur ajoutée forte s'étiole rapidement avec le temps.

Variété : la diversité ou l'hétérogénéité des données (données structurées ou non, texte, son, vidéo, journalisation, etc.) engendre la nécessité de disposer d'outils de traitement permettant de les appréhender pour donner du sens.

---

10 Michel Jaccard, De la protection des données à la sécurisation des données connectées ?, in : Regards de marathoniens sur le droit suisse, Mélanges publiés à l'occasion du 20ème « Marathon du droit », Genève 2015, p. 491 ss.

11 Michel Jaccard, *loc. cit.*, p. 496, étant précisé que Michel Jaccard se réfère à la définition de Gartner dans son glossaire IT : <http://www.gartner.com/it-glossary/big-data>.

12 Rolf H. Weber, Big Data : Sprengkörper des Datenschutzrechts, in : Datenschutz – Zum Aufstieg einer neuen Rechtsdisziplin, Berne 2015, p. 450 et 451.

13 <https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Big-Data-im-Praxiseinsatz-Szenarien-Beispiele-Effekte.html>.

14 The FOUR V's of Big Data, <http://www.ibmbigdatahub.com/infographic/four-vs-big-data>.

D'aucuns évoquent désormais une, voire deux abréviations supplémentaires[15] soit la véracité et la visibilité pour préciser les contours de cette activité.

Véracité : pour que la substantifique moelle des données puisse être extraite, il faut qu'elles soient de qualité ; au-delà de l'intégrité des données, la véracité des données permet une utilisation en pertinence.

Visibilité : elle doit permettre de bien utiliser les données et informations publiées en effectuant les recherches les plus pertinentes.

Un descriptif si long et précis des caractéristiques du Big Data est rendu nécessaire, car d'aucuns soutiennent que seules des données factuelles ou anonymisées sont collectées et que les dispositions relatives à la protection des données ne s'appliquent donc pas. Les prémices de la discussion doivent donc être techniques pour une bonne compréhension de la suite du raisonnement (confer ci-après § 2.1).

1.2 Le Big Data en Suisse

L'Office fédéral de la Communication (OFCOM) a mandaté la Haute école bernoise pour réaliser une étude[16] sur la thématique du Big Data visant à identifier les atouts et les risques du Big Data et d'établir les mesures prendre au niveau fédéral. Un sondage qualitatif a été diligenté auprès d'une vingtaine de spécialistes issus de l'économie, de l'administration et de la société civile, ainsi que sur un relevé quantitatif auprès de plus de 800 personnes de Suisse.

Selon cette étude, les questions les plus délicates ont trait à la protection des données personnelles et à la prévention contre une utilisation abusive des données. Différentes mesures sont préconisées telles qu'un changement de paradigme relativement au contrôle personnel sur les données ou encore l'implémentation de mesures de prévention des abus.

---

15 Guillaume Serries, Big Data, 3, 4 ou 5 V ?, article publié le 4 février 2016 sur le site ZDNet.fr : <http://www.zdnet.fr/actualites/big-data-3-4-ou-5-v-39832210.htm>.

16 L'étude en allemand est consultable à cette adresse : <https://www.egovernment.ch/dokumentation/studien/00189/index.html?lang=fr&p=1>.

En matière de données personnelles, l'étude préconise un accroissement du contrôle sur les données personnelles, ce par la définition de nouveaux droits de propriété et d'utilisation. Il est également fait référence à la nécessité de renforcer les règles de protection des données pour l'économie privée et d'intensifier, dans le cadre du droit de la concurrence, les contrôles sur les monopoles ou les quasi-monopoles dans le domaine de l'Internet et de prendre des mesures de sensibilisation. En sus, les conditions juridiques doivent être améliorées pour rendre les centres de données plus sûrs. Cette gouvernance des données doit être entreprise en collaboration avec l'économie privée et s'intégrer au contexte international. Les auteurs de l'étude parviennent également à la conclusion que, sous sa forme actuelle, le marché des données ne fonctionne pas (sic!) et que l'État doit donc s'engager fortement sans quoi l'évolution de la situation liée au Big Data va devenir immaîtrisable.

À la lecture de cette étude, on perçoit l'ampleur et le coût des démarches à accomplir pour que le Big Data ne se transforme pas d'ici quelques années en Bad Data[17]. Elle sonne comme un premier avertissement pour tous ceux qui considèrent que les données ne méritent qu'une polie et prudente autorégulation. Quant à l'urgence d'une action gouvernementale, elle est mise en exergue par le constat selon lequel le marché des données ne fonctionne pas. Une telle conclusion doit inciter à l'action tant politique que juridique, car cela signifie tout simplement qu'actuellement les données ne sont pas traitées avec le soin nécessaire, sans même entrer dans des considérations juridiques précises, ce qui sera le cas ultérieurement (cf. notamment § 2.1 ci-après).

Économiquement, la Suisse est souvent qualifiée de « Paradis du Big Data [18]» en raison du cumul de conditions-cadres favorables : fiabilité et faible coût de l'électricité, stabilité des conditions-cadres sur le plan économique, politique

17 Cf. à cet égard, Melissa Webster, White paper, Big Data, Bad Data, Good Data: The Link Between Information Governance and Big Data Outcomes, white paper sponsorisé par IBM et disponible à cette adresse : <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=WVL12376USEN>.

18 Matteo Maillar, La Suisse, paradis du big data, 21 juillet 2014 ; l'article est disponible à cette adresse : <http://www.largeur.com/?p=4207>.

et social, faibles risques naturels, caractère efficient des normes en matière de protection des données, licéité et absence de limite au cryptage, etc.

D'ici à cinq ans, les experts estiment que les internautes produiront 7 mégabytes de données par seconde[19]. Comme le relève Mathilde Farine dans son article, une telle quantité de données ouvrira un champ d'opportunités presque infinies pour les entreprises avec comme particularité désormais le fait que l'exploitation de données ne sera plus l'apanage de grandes entreprises, mais deviendra accessible à tous. Dans le domaine de la santé, cela signifie concrètement la possibilité de faciliter, respectivement d'affiner certains diagnostics. Longtemps sous-estimé le Big Data devient un enjeu économique majeur qui a fait dire à la Chancelière allemande Angela Merkel : « ceux qui voient les données comme une menace, ceux qui considèrent chaque donnée en termes de mauvaise utilisation qui peut en être faite, ne seront pas capables de saisir l'opportunité de la numérisation »[20]. Cet avertissement aux entreprises démontre que le marché a atteint un stade de maturité permettant la généralisation du Big Data dans la plupart des domaines d'activité et qu'il convient de s'y intéresser au plus vite. En termes juridiques, cette citation doit interpeller, car si comme le démontre l'étude précitée le marché des données n'est pas suffisamment régulé et que sa croissance s'accélère, il existe une forte probabilité qu'une lésion exponentielle des droits de chacun n'en résulte.

19 Mathilde Farine, L'exploitation du «big data» sera l'un des grands enjeux de 2016, éditorial, Le Temps du 27 décembre 2015, disponible ici : <https://www.letemps.ch/economie/2015/12/27/exploitation-big-data-sera-un-grands-enjeux-2016>.

20 Idem.

2 LA PROTECTION DES DONNÉES MÉDICALES

2.1 Le point de vue du Préposé fédéral à la protection des données[21]

« *Le public n'est pas suffisamment conscient des enjeux des «mégadonnées» (Big Data) et de la menace qu'elles représentent pour la sphère privée* »[22]. Cet article qui relate l'une des dernières prises de position du Préposé fédéral à la protection des données et à la transparence, M. Hans-Peter Thür confirme les craintes issues d'un développement rapide des services de Big Data sans régulation adéquate. Le Préposé préconise donc l'instauration d'une vraie stratégie digitale. Le grand public n'a pas suffisamment conscience des enjeux liés au Big Data, ce gigantesque réservoir d'informations personnelles générées par la révolution numérique[23].

Il convient de relever que le PFPDT s'était déjà exprimé en ce sens par le passé[24]. En mai 2013, il invitait à réviser la loi dans le domaine pour l'adapter à la réalité de la société de l'information en ces termes[25] : « *Le fait que, grâce aux algorithmes, l'on puisse désormais combiner des bases de données entre elles pour dresser le portrait d'un individu et prédire son comportement et ses besoins futurs m'inquiète. Lorsque j'ai pris mes fonctions en 2001, Internet n'avait pas le pouvoir qu'on lui connaît aujourd'hui. Google avait trois ans, Facebook et Twitter n'existaient pas. Désormais nous luttons contre le volume exponentiel de données générées par les réseaux sociaux, Internet ou la téléphonie mobile. On en mesure encore mal les conséquences. Les évolutions technologiques se greffent à cette problématique, car tous les outils qui permettent l'agrégation, l'enregistrement et l'analyse de ces données fragilisent davantage la sphère*

21 Abrégé ci-après PFPDT.

22 Le Temps du 29 juin 2015 : <https://www.letemps.ch/suisse/2015/06/29/heure-big-data-suisse-besoin-une-nouvelle-strategie-numerique>.

23 Idem.

24 Le Temps du 5 mai 2013 : <http://www.letemps.ch/suisse/2013/05/05/on-ne-mesure-impact-big-data-sphere-privee>.

25 Idem.

privée. À l'opposé, le Big Data est un formidable catalyseur d'idées et d'innovations. Tout cela est très ambigu. Mon défi consiste à favoriser le progrès tout en protégeant la sphère privée ».

Sur le plan strictement juridique, le PFPDT a publié différentes informations et recommandations qui peuvent se résumer ainsi[26].

La première question qui se pose a trait à l'application de la loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1 ; abrégée ci-après LPD)[27]. Ainsi que le relève le PFPDT, un argument souvent invoqué dans le contexte des données massives est que, dans la plupart des cas, seules des données factuelles ou anonymisées sont collectées et que les dispositions relatives à la protection des données ne s'appliqueraient donc pas. Rappelons à cet égard que les normes en matière de protection des données ont été conçues pour régler le traitement de données liées à une personne[28]. En l'occurrence, il ne saurait être exclu que par rapprochement de collections de données il soit possible de parvenir à une désanonymisation, ce qui justifie l'application de la LPD. Le Préposé ajoute que « *Dans de nombreux cas, l'anonymisation des identificateurs particuliers évidents ne suffit pas à exclure toute réidentification. Même les quasi-identificateurs - des combinaisons d'attributs, comme la date de naissance, le sexe et le code postal - doivent être traités avec précaution* ». Il fonde notamment sa démonstration sur des travaux réalisés par des scientifiques américains au terme desquels il a été établi que les quatre cinquièmes de la population américaine pouvaient être identifiés a posteriori sur la seule base de ces trois caractéristiques (date de naissance, sexe et code postal). La règle qui s'applique est donc la suivante : dans l'hypothèse d'une anonymisation des données insuffisante, les exigences en matière de traitement prévues par la législation relative à la protection des données s'appliquent et le maître du fichier d'origine peut devoir être amené à rendre des

26 <http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=fr>.

27 <https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html>.

28 Selon l'article 3 alinéa 1er LPD sont considérées comme données personnelles toutes les informations qui se rapportent à une personne identifiée ou identifiable.

comptes. La situation devra donc être appréciée *in concreto*, ce qui paraît pertinent compte tenu des développements rapides en cette matière.

À cela s'ajoute le fait que l'évolution technologique prévisible rendra possible une attribution à une personne déterminée des données notamment par l'adjonction de nouvelles sources, ce qui générerait une grave violation des droits de la personnalité. Le PFPDT émet en conséquence une première recommandation : examiner les questions liées à la protection des données dès le développement de nouvelles technologies en intégrant la protection des données à la conception d'ensemble *ab initio* « *Privacy by Design*[29] ». Sommes toutes, il s'agit de l'application des principes de prévention et de précaution qui peuvent paraître évidents, mais qui, d'expérience, ne sont pas les premiers soucis lors du développement d'une infrastructure informatique. Bien au contraire, puisque c'est avant tout la performance qui constitue le but ultime du Big Data : générer une forte valeur ajoutée et permettre une recherche topique. Les objectifs du régulateur et des développeurs sont donc par nature antinomiques.

En ce qui concerne l'exigence de transparence prévue par la loi, le PFPDT considère que chacun est en droit de savoir quelles sont les données le concernant qui sont traitées, par qui et dans quel but. L'un des problèmes du Big Data, de ce point de vue, a trait à l'opacité tant du traitement que de la connexion de données issues de sources diverses. Il en résulte une quasi-impossibilité de vérification par les personnes concernées. Chaque utilisateur doit donc se montrer très vigilant selon le PFPDT. Cette vigilance pourrait se manifester, avant le choix d'un prestataire, par des questions ciblées portant sur l'origine des données, le but précis de leur traitement et leur pérennisation. Il s'agirait en quelque sorte pour user d'une métaphore alimentaire de s'assurer de l'existence de « données d'origine contrôlée ». Il est vrai, cependant, que le client potentiel sera bien incapable de vérifier que les déclarations à lui émises sont conformes à la réalité, surtout si le prestataire de ser-

[29] Pour de plus amples informations relativement à ce principe, cf. Agnès Hertig Pea, La protection des données médicales est-elle efficace ?, Neuchâtel 2013, p. 302.

vice se trouve à des milliers de kilomètres. Il convient donc d'opter, à performances égales, pour un prestataire suisse pour lequel le régime légal est connu et dont les éventuels manquements pourront faire l'objet d'une action dans notre pays à des conditions prévisibles, car parfaitement définies par la loi.

Le traitement de données massives à caractère personnel requiert le consentement[30] des personnes concernées. Le but des procédures impliquant des données massives doit pouvoir être reconnu clairement et sans ambiguïté par les personnes concernées, et ce, dès la collecte des données. Cette approche contredit toutefois le principe fondamental de fonctionnement des données massives, celles-ci impliquant naturellement la constitution de stocks de données, lesquels serviront ultérieurement à un but encore indéterminé. Fournir à titre d'information une description ouverte, générale, du but du traitement des données engendre l'invalidité juridique du consentement au traitement prévu. En clair, le consentement ne pourra jamais être donné valablement dès lors que le but n'est pas déterminable sur la durée. Il apparaît également difficile lorsqu'une révocation du consentement a été émise de pouvoir s'assurer de l'effacement définitif des données.

L'exigence de l'exactitude des données[31] constitue un écueil supplémentaire : les algorithmes appliqués aux données massives analysent de grandes masses de données de manière autonome, automatisée, à la recherche notamment de corrélations. Ces procédures d'analyse créent nativement de nouvelles informations liées à des personnes, sans qu'il soit possible de les qualifier d'exactes ou de fausses, puisqu'elles ne constituent que des probabilités ou des interprétations. Ainsi, il est théoriquement possible, à l'aune de mon dossier médical, que je sois considéré comme une personne présentant un risque cardiaque élevé et catalogué ainsi, sans même le savoir.

30 Cf. article 4 al. 5 LPD et Agnès Hertig Pea, loc. cit., p. 143 ss et les nombreuses références citées.

31 Cette exigence est prévue à l'article 5 LPD ; cf. également Agnès Hertig Pea, loc. cit. p. 99 et les références citées.

Le PFPDT termine son analyse en ces termes : « *De ce fait, un examen approfondi de la LPD s'impose, pour déterminer si les principes essentiels que sont l'assignation d'un but précis, le consentement des personnes concernées et la transparence peuvent être respectés lors de l'utilisation de données massives*[32] ». En clair, le régime juridique actuel doit faire l'objet d'une analyse approfondie, aux fins d'établir s'il est en capacité de répondre aux défis du Big Data, analyse qui, comme nous le verrons ci-après[33], devra curieusement encore attendre.

2.2 Perspectives législatives

Le Conseiller national Paul Rechsteiner a déposé le 26 septembre 2013 une motion (13.3841) intitulée « Commission d'experts pour l'avenir du traitement et de la sécurité des données »[34]. Voici le libellé précis de cette motion :

Le Conseil fédéral est chargé, pour l'avenir du traitement et de la sécurité des données, d'instituer une commission d'experts interdisciplinaire devant répondre aux questions suivantes:

1. D'un point de vue technologique et politique, comment évaluer l'état actuel du traitement des données?

2. Quels sont les effets sur l'économie suisse, la société et l'État?

3. Comment évaluer le cadre juridique actuel dans ce domaine?

4. Quelles conclusions en tirer pour la Suisse au niveau national? Quelles conclusions en tirer quant à d'éventuelles initiatives au niveau international?

---

32 Pour ceux que cette brève synopsis ne satisferait pas, il convient de signaler que le PFPDT ad interim M. Jean-Philippe Walter a donné une conférence sur cette thématique le 7 mai 2015 à Lausanne et que sa présentation très complète est accessible ici : <http://docplayer.fr/3293208-Prepose-federal-a-la-protection-des-donnees-et-a-la-transparence-pfpdt-la-protection-des-donnees-a-l-heure-des-megadonnees-big-data-big-protection.html>.

33 Cf. § 2.2.

34 La motion et la réponse du Conseil fédéral sont disponibles à cette adresse : <http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20133841>.

Le Conseil fédéral a proposé le rejet de la motion le 20 novembre 2013, arguant notamment du fait que l'institution d'une telle commission ferait double emploi avec l'activité déployée dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC[35]) du 27 juin 2012. Le Conseil fédéral estime dès lors que les connaissances nécessaires, les recommandations et les mesures requises sont déjà assurées par la SNPC, par les directives en vigueur ainsi que par la future loi sur la sécurité de l'information. Il concède toutefois, dans sa réponse, qu'une révision de la loi fédérale sur la protection des données est pertinente, car les menaces dans ce domaine se sont accrues depuis quelques années en raison des développements technologiques et de l'évolution de la société et a donc chargé le Département fédéral de justice et police d'examiner des mesures législatives visant à renforcer la protection des données[36]. Cette prise de position n'a pas convaincu puisque le parlement a imposé en 2014 au Conseil fédéral de mettre sur pied une commission d'experts chargée de poser des jalons pour une nouvelle politique en matière de traitement et de sécurité des données personnelles. Cette commission doit livrer ses premières conclusions d'ici à fin 2017. Il va sans dire que ces conclusions sont très attendues. D'autant plus attendues, que la thématique du Big Data n'a pas été évaluée par le groupe d'accompagnement révision LPD ! En fait, suite à la saisine du DFJP par le Conseil fédéral, des travaux d'évaluation de la LPD ont été conduits en 2010 et 2011 par un groupe de travail élargi[37]. Ces travaux ont abouti à un rapport final[38] ayant servi de base au rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données du 9 décembre 2011[39], rapport au terme duquel il chargeait le DFJP d'examiner l'opportunité de renforcer la législation en matière de protection des données et de faire des propositions

35 FF 2013 517.

36 Nous y reviendrons ci-après.

37 Dont le soussigné était membre.

38 Pour de plus amples informations, cf. <https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html>.

39 Le rapport est disponible à cette adresse : <https://www.admin.ch/opc/fr/federal-gazette/2012/255.pdf>.

concernant la marche à suivre avant la fin de 2014, à l'aune des résultats de l'évaluation et des développements en cours au sein de l'UE et du Conseil de l'Europe. Pour bénéficier de l'expertise nécessaire et pour tenir compte des intérêts des différents groupes de personnes concernés par une éventuelle révision de la loi sur la protection des données[40], l'Office fédéral de la justice (OFJ) a instauré un groupe d'accompagnement qui s'est penché de septembre 2012 à octobre 2014 sur les mesures législatives à prendre. Le rapport du groupe d'accompagnement[41] intitulé « *Esquisse d'acte normatif relative à la révision de la loi sur la protection des données - Rapport du groupe d'accompagnement Révision LPD* » a été rendu le 29 octobre 2014. Le Conseil fédéral en a pris connaissance le 1er avril 2015 et il a donné le coup d'envoi d'une révision de la LPD en sollicitant du DFJP qu'un avant-projet de loi lui soit soumis avant fin août 2016, lequel devra tenir compte des réformes en cours dans l'UE et au Conseil de l'Europe[42].

Le Conseil de l'Europe opère une refonte de la convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[43]. Le projet de modernisation de cette convention sera sans doute adopté et soumis à la signature des États parties en 2016[44]. Or renoncer à ratifier la nouvelle convention aurait, de l'avis du Conseil fédéral, des con-

---

40 Le DFJP a donc mis sur pied un groupe de travail ayant une large assise, composé de représentants des administrations fédérales et cantonales, des milieux scientifiques, des organisations économiques et des associations de défense des consommateurs.

41 Disponible à cette adresse: <https://www.bj.admin.ch/content/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-f.pdf>.

42 <http://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2015/2015-04-010.html>.

43 Ratifiée par la Suisse.

44 Pendant la seconde phase de la modernisation – qui commence en 2016 – le comité intergouvernemental d'experts élaborera une proposition finale qui assurera la cohérence avec le nouveau règlement et la directive de l'UE concernant la protection des données. Le protocole portant révision de la Convention sera en fin de compte soumis au second semestre pour adoption au Comité des Ministres. Cf. également : <https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2016)WP2016-2017_Programme%20de%20travail_25%2009%202015.pdf>.

séquences fâcheuses importantes sur le trafic international de données. L'UE, elle aussi, modifie sa législation relative aux données personnelles par l'adoption d'un Règlement général sur la protection des données et une Directive sur la protection des données traitées à des fins répressives lesquels devraient entrer en vigueur au printemps 2018[45]. La Suisse n'est concernée que dans la mesure où ces actes normatifs relèvent de l'acquis de Schengen/Dublin, mais les échanges de données avec l'UE reposent en principe sur le fait que le niveau de protection des données garanti par la Suisse est reconnu comme adéquat. La Suisse a donc un intérêt majeur à renforcer ses dispositions selon le Conseil fédéral.

La révision de la LPD devrait, selon les vœux du Conseil fédéral, mettre la Suisse en état de ratifier la nouvelle convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de reprendre si nécessaire les développements de l'acquis de Schengen/Dublin en matière de protection des données. C'est la raison pour laquelle un délai si bref a été octroyé au DFJP pour présenter un avant-projet.

Le processus étant exposé, examinons plus avant ce que contient le rapport groupe d'accompagnement intitulé « *Esquisse d'acte normatif relative à la révision de la loi sur la protection des données* » relativement au Big Data.

La lecture du rapport réserve une surprise de taille, puisque le Big Data n'a pas été traité de manière directe et exhaustive : « *La présente esquisse d'acte normatif ne s'attache en revanche pas en détail au thème du Big Data (méga-données ou données massives*) [46]». Le groupe d'accompagnement justifie cette décision en arguant du fait que les conséquences du Big Data ne sont pas encore bien connues et que la doctrine juridique n'a traité en détail que quelques aspects de cette problématique. En conséquence, des solutions globales ne sont pas proposées, mais uniquement des mesures ponctuelles qui

45 <http://www.consilium.europa.eu/fr/press/press-releases/2015/12/18-data-protection/#>.

46 Rapport du groupe d'accompagnement Révision LPD « *Esquisse d'acte normatif relative à la révision de la loi sur la protection des données* » du 29 octobre 2014, p. 7.

permettent de s'attaquer aux défis posés par le Big Data en matière de protection des données. Voici les mesures ponctuelles évoquées[47] :

- Propositions de réglementation relatives au Privacy by Design ;
- Propositions de réglementation relatives à l'analyse de l'impact potentiel du traitement de données ;
- Propositions de réglementation relatives au droit d'accès relatif à la structure logique du traitement des données ou aux décisions individuelles automatisées.

Pour le groupe d'accompagnement, un examen approfondi des implications du Big Data pour la protection des données pourrait[48] intervenir dans le cadre des travaux de mise en œuvre de la motion Rechsteiner, dont les premières[49] conclusions sont attendues pour la fin de l'année 2017, autrement dit dans le monde de l'informatique régi par les lois de Gordon E. Moore[50], une éternité !

Comme le relève le PFPDT dans son rapport annuel 2014/2015[51], si nous voulons influencer le cours des choses, les règles doivent être rapidement adaptées, sinon le développement technique nous placera devant le fait accompli. Il est désormais évident que cette thématique sera régie par une appréhension *a posteriori* d'une normalisation technique qui laisse augurer de nombreux problèmes en termes de protection des données. Le PFPDT déclarait lors de la présentation de son rapport annuel 2014/2015[52] : « *J'espère vivement que la Commission Rechsteiner, qui doit livrer ses résultats d'ici la fin de l'année 2017, donnera un élan important qui se manifestera également dans la révision de la loi sur la protection des données (LPD)* ».Or, avec le désir affiché

47 À titre exemplatif.

48 Le conditionnel n'augure aucune garantie de traitement de cette thématique.

49 Mis en exergue par le soussigné.

50 <https://fr.wikipedia.org/wiki/Loi_de_Moore>.

51 22ème rapport d'activité 2014/2015, p. 7.

52 Idem, p. 8.

du Conseil fédéral de donner une impulsion décisive à la révision de la LPD cette année encore, peut-être sera-t-il trop tard pour intégrer les résultats de la Commission Rechsteiner, alors que le Big Data eût pu faire l'objet d'une analyse détaillée par le groupe d'accompagnement. Il s'agit sans nul doute d'une occasion manquée dont nous pourrons mesurer les conséquences d'ici à deux ans. Ce choix opéré est d'autant plus incompréhensible que le PFPDT a régulièrement, depuis 2 ans, axé sa communication préventive sur cette thématique et qu'une résolution a été adoptée lors de la Conférence internationale des commissaires à la protection des données et à la vie privée qui s'est déroulée du 13 au 17 octobre 2014 à l'Île Maurice, conférence à laquelle la Suisse participait[53] : *Une résolution sur les mégadonnées appelant tous les acteurs du «big data» à respecter les principes de protection des données, notamment la limitation des finalités, le principe de proportionnalité, les obligations de transparence des traitements et la garantie des droits de personnes concernées (droit d'accès, information, droit de rectification ou d'effacement des données).*

Les attentes placées dans les travaux de la Commission Rechsteiner sont ainsi aussi incommensurables que le Big Data[54] !

2.3 Brève revue de la doctrine récente

Le Big Data mobilise les énergies et les neurones, puisqu'un ouvrage topique paraît en mars[55] et que deux auteurs y ont consacré un article récemment.

---

53 Idem, p. 73 et 74.

54 Le Professeur Bertil Cottier, membre du groupement d'accompagnement s'est exprimé ainsi relativement à la suppression dans la LPD de la notion de « profil de la personnalité » au moment où les nouvelles technologies de l'information permettent la prise de décisions ayant des effets juridiques sur la base de profilage d'informations reposant sur des données statistiques : « *C'est une norme typique de la loi suisse de protection des données qui aurait exigé un examen approfondi, car les collectes du « Big Data » correspondent exactement à la notion de profil de personnalité. Ce problème a été réglé trop vite et nécessiterait un réexamen* », Interview de Bertil Cottier sur le projet de révision de la LPD, in : plaidoyer 1/16, p. 16.

55 Cet article a été écrit en février 2016 et pour l'ouvrage : Astrid Epiney / Daniel Nüesch, Big Data et droit de la protection des données, ouvrage à paraître en mars 2016 chez Schulthess :

Michel Jaccard[56] considère tout d'abord que si les atouts du Big Data sont indéniables, les menaces le sont tout autant[57]. Selon lui, les principes actuels de la protection des données ne sont pas adéquats pour traiter ces nouveaux risques, car les normes visent à protéger un individu ou une personne morale notamment en termes de consentement, alors que dans une approche Big Data, la collecte des données intervient sans que la finalité ne soit nécessairement connue, intrinsèquement sans que celle-ci soit connue selon la définition retenue par le PFPDT. Des démarches ultérieures à la collecte, tel que mise en relation ou comparaison peuvent permettre sur la base d'informations fragmentaires (sexe, date de naisse et code postal) de procéder à une identification. Ainsi, des données non couvertes par les lois en matière de protection des données, voire totalement anonymes pourraient générer des conséquences importantes sur la vie privée des gens, respectivement léser leurs droits de la personnalité. L'auteur considère qu'il est donc possible d'envisager dans quelques années un monde de smart data sur cette base. Il préconise une approche différenciée fondée sur un certain type de traitements (par comparaison et recoupement), plutôt que l'approche actuelle qui se fonde sur le caractère personnel ou non des données. À cet égard, nonobstant la définition large des données personnelles et son extension jurisprudentielle[58], de nombreuses données collectées dans le cadre du Big Data n'en feraient pas partie, alors que par leur recoupement une identification est

<https://www.schulthess.com/verlag/detail/ISBN-9783725574148/Epiney-Astrid-Hrsg.-Nueesch-Daniela-Hrsg./Big-Data-und-Datenschutzrecht--Big-Data-et-droit-de-la-protection-des-donnees>.

56 Michel Jaccard, De la protection des données à la sécurisation des données connectées ?, in : Regards de marathoniens sur le droit suisse, Mélanges publiés à l'occasion du 20ème « Marathon du droit », Genève 2015, p. 491 ss.

57 L'auteur se réfère notamment à une publication de mai 2014 de l'Executive Office du Président des États-Unis, intitulée « Seizing opportunities, preserving values, disponible ici : <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

58 Sont désormais des données personnelles, les adresses email, les cookies, l'historique de navigation, l'adresse IP (arrêt non publié 1C_285/2009), ou les données géolocalisées.

possible. La LPD n'est donc plus adaptée[59] et l'extension de son champ d'application insuffisante (par une nouvelle définition plus large de la notion de données personnelles), car non susceptible d'appréhender correctement la réalité de l'échange des données notamment en termes de consentement, à l'instar de l'échange des données entre objets connectés. La législation devrait donc évoluer dans le sens d'une plus grande flexibilité pour ce qui concerne les exigences relatives au but du traitement et à la transparence : tout traitement ultérieur qui ne serait pas incompatible avec le traitement original serait autorisé. À l'aune de l'évolution de la législation américaine, l'auteur considère également que la notion de « *contexte* » fera prochainement l'objet de discussions, l'idée étant qu'une personne ne pourrait se plaindre *a priori* d'un traitement de données effectué dans un contexte envisageable au moment de la collecte[60]. Cela équivaudrait donc à introduire une sorte d'*opt-out* pour les situations prévisibles de traitements de données avec une information assez large et vague et réserver les cas d' « *opt-in* » avec un consentement spécifique aux seules situations qui visent un traitement de données sensibles. La contrepartie pourrait consister en un renforcement des obligations imposées aux responsables de traitement : *data minimization*[61], *privacy by design*[62], *privacy by default*[63], droit à l'oubli[64]…

Rolf H. Weber[65] considère, quant à lui, qu'il sera toujours plus difficile, à l'avenir, de distinguer les données personnelles des données factuelles. Pour

59 La LPD s'applique toutefois à la « pseudo-anonymisation » et l'anonymisation elle-même constitue un traitement de données soumis à la loi (art. 13 al. 2 let. e LPD).

60 Même sans être clairement défini.

61 Obligation générale de minimiser l'utilisation des données personnelles et leur durée de conservation.

62 Nécessité d'intégrer la protection des données dès la conception.

63 Obligation de fournir aux personnes concernées les moyens de mieux contrôler les paramètres des traitements de leurs données personnelles et établissement par défaut du niveau de traitement le moins intrusif.

64 Obligation de garantir un droit à l'effacement des données personnelles conservées qui n'équivaut pas à un réel droit à l'oubli.

65 Rolf H. Weber, Datenschutz – Zum Aufstieg einer neuen Rechtsdisziplin, Bern 2015, ouvrage qui comporte deux articles consacrés au Big Data : Big Data : Sprengkörper des Datenschut-

ce seul motif, il paraît pertinent d'édicter des dispositions légales spécifiques pour certains secteurs tels que l'eHealth, où les avantages et les risques du Big Data sont particulièrement marqués. Il serait également envisageable de formuler des propositions de régulations, respectivement de prohiber la publication de données anonymisées dans l'hypothèse où le risque de désanonymisation est considérable. Aux fins de réduire les asymétries existantes en termes d'information entre la personne chargée du traitement des données et les individus, il est essentiel de créer une plus grande transparence par le biais du consentement ou par une implémentation du principe d'accountability (Accountability – Standard)[66]. Finalement selon Rolf H. Weber, il convient de plaider pour un renforcement du concept d' « Identity Centrics », de manière à ce que les individus reprennent le contrôle de leurs données et qu'il leur soit plus aisé de procéder à un effacement de données. Il prône que les entreprises investissent plus d'argent dans la sécurité de leurs données. La protection des données pourrait à l'avenir devenir un label de réputation[67] pour les entreprises. Dans l'hypothèse où cet aspect devenait un argument concurrentiel entre entreprises, certains problèmes pourraient être *de facto* réglés. Quoi qu'il en soit, le consentement tel qu'il est prévu à l'article 13 LPD n'est plus approprié en ce qui concerne le Big Data.

La notion d' « Accountability » évoquée par Rolf H. Weber est intéressante. Il s'agit d'une obligation de rendre compte et d'expliquer, avec une idée de transparence, et de traçabilité permettant d'identifier et de documenter les mesures mises en œuvre pour se conformer aux exigences issues de la réglementation[68]. Elle sous-tend également l'obligation de responsabilité touchant à l'idée, pour le responsable de traitement, d'être garant d'un résultat, de

zrechts ? p. 449 et Aushölung des Datenschutzes durch De-Anonmymisierung bei Big Data Analytics, p. 467, étant précisé que cet article a été écrit avec Dominic Oertly.

66 <http://network.lexing.eu/accountability-et-protection-des-donnees-personnelles/>.

67 A l'instar de ce qui se passe en France.

68 Chloé Torres, Accountability et protection des données personnelles, article publié le 24 octobre 2012, accessible ici : <http://network.lexing.eu/accountability-et-protection-des-donnees-personnelles/>, Me Chloé Torres évoque la réglementation Informatique et libertés, le pendant français de notre LPD.

l'effectivité de la protection des données et de la vérifiabilité des mesures prises. Ce principe implique donc non seulement l'obligation du responsable du traitement de se conformer aux règles applicables, mais également celle de pouvoir démontrer aux autorités ou aux personnes concernées comment il s'y tient[69].

L'article 22 du règlement européen[70] visant à réformer la directive n° 95/46/CE relative à la protection des données à caractère personnel impose, en effet, au responsable du traitement d'adopter des règles internes et de mettre en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect de la réglementation.

La mise en pratique du principe d'accountability en matière de protection des données se traduit ainsi notamment par[71] :

- la mise en place de procédures efficaces pour assurer la conformité de l'entreprise avec la réglementation ;
- la mise en place d'une politique SIF (sensibilisation- information-formation) en matière de protection des données à l'attention du personnel ;
- la réalisation d'un audit destiné à évaluer le niveau de conformité des traitements mis en œuvre à la réglementation et à identifier les mesures correctives à implémenter afin de réduire les écarts de conformité ;
- la mise en place d'une équipe dédiée en matière de protection des données (data privacy officer, etc.) ;

69 Idem.

70 Le règlement devrait entrer en vigueur au printemps 2016 et sera d'application à compter du printemps 2018 ; <http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=fr>.

71 Idem, étant précisé que le soussigné a adapté le texte en supprimant les références du droit français.

- l'adoption de l'approche Privacy by Design ;
- l'adoption et l'implémentation de Binding Corporate Rules pour encadrer les flux transfrontières de données ;
- la tenue d'une documentation sur les traitements effectués ;
- la réalisation d'une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel.

Ce principe pourrait donc se révéler extrêmement utile s'agissant du Big Data pour lequel des cautèles supplémentaires s'avèrent de l'avis unanime de la doctrine et du PFPDT nécessaires.

3 LE BIG DATA EN MATIÈRE DE DONNÉES MÉDICALES

3.1 Introduction

Ainsi que le relève le Préposé fédéral, les données de santé restent un domaine ultrasensible[72]. Au cours de l'année écoulée[73], les services de Hanspeter Thür ont attiré l'attention des médecins sur les risques présentés par la conservation des données de leurs patients dans un nuage informatique[74]. Le PFPDT s'est également opposé à certaines dispositions du projet de loi visant à créer un registre national des maladies oncologiques. La dernière mouture soumise par le Conseil fédéral au parlement, qui prévoit d'enregistrer les cas sous le numéro AVS du malade, ne satisfaisait toujours pas Hanspeter Thür. Selon lui, cette procédure « présente de gros risques » en raison des connexions qu'elle permet d'établir entre différentes bases de données. Et pourrait-on ajouter des corrélations qui peuvent ainsi être établies…

72 Le Temps du 29 juin 2015, <https://www.letemps.ch/suisse/2015/06/29/heure-big-data-suisse-besoin-une-nouvelle-strategie-numerique>.

73 2014/2015.

74 Il leur a été conseillé de s'assurer que des tiers ne peuvent y avoir accès pour les traiter.

En matière médicale, les principes évoqués par le Préposé dans son analyse du Big Data[75] revêtent une importance particulière. Ne serait-ce que du fait que ces données relatives à la santé sont légalement considérées comme des données sensibles[76] et qu'elles bénéficient d'une protection accrue. Il s'agit d'une catégorie de données méritant intrinsèquement une protection particulière, du fait de l'impact particulièrement important qu'elles peuvent avoir, de par leur nature ou leur fonction, sur la personnalité. Elles sont ainsi des données susceptibles *per se* de porter atteinte aux libertés fondamentales ou à la vie privée[77]. La protection accrue pour ce genre de données se justifie entre autres par le fait que leur traitement est susceptible de générer des discriminations. L'effet doit donc être préventif : si le maître du fichier est tenu d'informer la personne de manière plus étendue que pour d'autres types de données, respectivement exhaustivement, il aura tout intérêt à s'abstenir de traiter les données sensibles ou les profils de la personnalité dont il n'a absolument pas besoin pour remplir ses tâches.

Les données relatives à la santé, qui font partie de la sphère intime, ont été mentionnées séparément dans la LPD, vu leur importance[78]. Ont été considérés comme revêtant cette qualité, les propos échangés dans le cadre d'une psychothérapie[79], les données médicales d'une employée[80], les résultats d'une analyse de sang[81] ou encore une déclaration d'aptitude ou d'inaptitude émise par un médecin[82].

Les données massives sont d'ores et déjà utilisées, croisées, et agrégées pour déterminer l'avancée d'une épidémie ou encore décider de l'acceptation d'un

75 Cf. § 2.1 ci-avant.

76 Cf. article 3 let. c LPD.

77 Cf. consid. 33 du Préambule à la Directive 95/46.

78 ATF 130 III 33.

79 PFPDT, Rapport 1998/1999, p. 336.

80 ATF 119 II 222 (225) consid. 2b/aa.

81 Arrêt non publié 4C.192/2001 du 17 octobre 2001, consid. 2b/aa, X. SA contre Y.

82 Christian Flueckiger, Dopage, santé des sportifs professionnels et protection des données médicales, Bâle 2008, p. 59.

nouvel assuré. Google teste par exemple depuis 2014 un service de consultation médicale en ligne[83]. Lorsque vous tapez « douleur au genou » le moteur offrirait alors la possibilité d'ouvrir une fenêtre de chat vidéo avec un médecin pour en savoir plus. Ce service disponible aux États-Unis et initialement gratuit serait destiné à devenir onéreux une fois généralisé. Les exemples sont légion[84].

Il va très rapidement devenir nécessaire de fixer de nouvelles conditions d'exercice des professions médicales, en termes de sécurité des données. Ainsi, les médecins devraient-ils devoir intégrer dans les contrats qui les lient à leurs prestataires informatiques une clause spécifiant qu'en cas de rupture contractuelle, les données-patient soient restituées à très brève échéance pour éviter toute mise en danger. Dans une récente affaire valaisanne, ubuesque, des patients n'ont plus eu accès à leurs données médicales pendant deux semaines[85], suite à un litige tripartite entre médecins et fournisseur informatique. Tout ceci n'a pas lieu d'être et il faudra se résoudre à des démarches d'habilitation ou à des mesures coercitives à intégrer dans les normes en matière de santé publique pour éviter que la partie de surcroît la plus faible soit le patient ne soit contrainte de subir un quelconque désagrément du fait du recours aux technologies de l'information qui devraient pour lui représenter une chance supplémentaire de guérir. Dans ce contexte, les organisations professionnelles doivent empoigner ce problème participer au débat en assistant les professionnels de la santé, bien désarmés faut-il le préciser devant les nouvelles exigences de régulation qui vont les assaillir et pour lesquelles, ils n'ont souvent pas été formés.

---

83 <http://www.huffingtonpost.fr/2014/10/13/sante-google-chat-medecins-internautes_n_5975310.html>.

84 Revue médicale suisse, Interview de Amalio Telenti, La médecine face à la révolution numérique, 2015, p. 940 à 943 ; Didier Trono, Le Big Data au service de la génomie, in : Revue de la société vaudoise de médecine, novembre 2015, p. 4 et 5.

85 <http://www.lenouvelliste.ch/articles/valais/valais-central/des-patients-sierrois-n-ont-plus-acces-a-leurs-donnees-medicales-depuis-deux-semaines-449285>.

Aux États-Unis, des budgets importants ont été consacrés à la standardisation des dossiers médicaux électroniques. Dans notre pays les sommes consacrées sont infinitésimales, de sorte que les médecins ne peuvent rien attendre de l'État et doivent s'organiser pour faire face à un défi qu'ils ne pourront relever chacun dans leur cabinet.

Nous sommes tous des embryons du Big Data, raison pour laquelle, une attention particulière doit être vouée à cette thématique[86] dans le domaine médical.

TA-SWISS[87], soit le Centre d'évaluation des choix technologiques a récemment mis récemment au concours[88] une étude interdisciplinaire relative au « *quantified self* » dont le but est d'en évaluer les opportunités et les risques. Sur le plan juridique, les questions principales ont trait à l'identification des personnes, la titularité des données, le respect de la sphère privée, ainsi que les dispositions complémentaires à adopter en matière de protection des données et de propriété intellectuelle. Au terme de cette étude, une vision plus claire devrait émerger sur le plan fédéral.

3.2 Le dossier électronique du patient[89]

Le dossier médical informatisé du patient[90] est l'une des composantes d'un sous-groupe de domaine appelé « e-Health » ou « Cybersanté » qui regroupe les activités ayant recours à l'utilisation des technologies de l'information et

86 Sébastien Fanti, « Nous sommes tous des embryons du Big Data », in : Le Temps du 4 septembre 2015, disponible ici : <https://www.letemps.ch/suisse/2015/09/04/sebastien-fanti-sommes-embryons-big-data>.

87 <https://www.ta-swiss.ch/fr/>.

88 Cf. Newsletter 4/2015 de TA-SWISS.

89 Un audit étant actuellement en cours relativement au dossier électronique du patient dans le Canton du Valais, le soussigné s'abstiendra de commenter les choix opérés à cet égard et se limitera à une analyse juridique des normes cantonales, dans le respect de son devoir de réserve ; un rapport sera publié à cet égard.

90 Ce dossier médical informatisé se distingue du dossier électronique du patient régi par la loi éponyme.

de la communication[91] « *pour l'organisation, le soutien et la mise en réseau de tous les processus et acteurs du système de santé*[92] ». S'inscrivent notamment dans ce concept très général, la télémédecine, la cybermédication, la création de banques de données médicales ou la mise en réseau des acteurs de soins.

Le contexte de l'informatisation des dossiers patients en Suisse s'inscrit dans le cadre de la stratégie nationale en matière de cybersanté (e-Health[93]), stratégie adoptée en juin 2007. L'intention du Conseil fédéral était de mettre en place une stratégie afin de contribuer à garantir à la population l'accès à un système de santé qui allie qualité, efficience de sécurité[94].

En septembre 2007, le Département fédéral de l'intérieur (DFI) et la Conférence suisse des directrices et directeurs cantonaux de la santé (CDS) ont signé une convention-cadre de droit public régissant la collaboration entre la Confédération et les cantons en vue de mettre en œuvre la Stratégie Cybersanté Suisse. À cette occasion, ils ont convenu de créer un organe de coordination en matière de Cybersanté. C'est ainsi qu'est née « e-Health Suisse[95] », une entité chargée principalement d'élaborer des recommandations en vue

91 Sabrina Burgat, Carte d'assuré dossier patient informatisé, E-Health : récents développements, in : Olivier Guillod, Protection des données médicales et transparence… du patient ? Berne 2012, p. 55.

92 Voir le rapport intitulé « Stratégie Cybersanté (e-health) Suisse du 27 juin 2007 élaboré par le Département fédéral de l'intérieur, disponible à cette adresse : <http://www.bag.admin.ch/themen/gesundheitspolitik/10357/index.html?lang=fr>.

93 Par eHealth ou cybersanté on entend l'utilisation des TIC pour l'organisation, le soutien, la mise en réseau et l'infrastructure des processus et partenaires, inclus les patients, impliqués dans le système de santé, Christian Lovis / Antoine Geissbühler, Dossier médical informatisé et cybersanté, in : Dominique Bertrand, Jean-François Dumoulin, Romano La Harpe, Marinette Ummel, Médecin et droit médical, Présentation et résolution de situations médico-légales, 3ème édition, p. 166.

94 Christian Lovis / Antoine Geissbühler, Dossier médical informatisé et cybersanté, in : Dominique Bertrand, Jean-François Dumoulin, Romano La Harpe, Marinette Ummel, Médecin et droit médical, Présentation et résolution de situations médico-légales, 3ème édition, p. 166 ss.

95 <http://www.e-health-suisse.ch/index.html?lang=fr>.

de coordonner, au niveau national, la mise en réseau des acteurs du système de santé[96].

Le 3 décembre 2010, dans le cadre de la stratégie « e-Health » le Conseil fédéral a chargé le DFI d'élaborer l'avant-projet relatif aux règlementations nécessaires à l'introduction, à la diffusion et au développement d'un dossier électronique du patient. Cet avant-projet a été mis en consultation du 16 septembre au 20 décembre 2011 et les prises de position des milieux intéressés ont été rendues publiques durant l'année 2012.

Dans son avant-projet, le législateur avait opté pour la création d'un cadre législatif permettant l'introduction d'un dossier électronique du patient, sans toucher à la réglementation en matière de protection des données[97], ce qui explique certaines difficultés dont il sera question ci-après (notamment l'absence de prise en considération initiale de cette thématique). Concrètement, cela signifie que les questions de protection des données continuent d'être réglées par les dispositions légales fédérales et cantonales actuelles[98].

Cet avant-projet a donc servi principalement à fixer les conditions juridiques et techniques qui doivent permettre aux professionnels de la santé d'échanger des données médicales pertinentes. Singulièrement, les recommandations techniques ne figuraient pas dans l'avant-projet de loi, nonobstant, notamment, le rapport consacré aux normes et architectures qui contenait des re-

96 Sabrina Burgat, Carte d'assuré dossier patient informatisé, E-health : récents développements, in : Olivier Guillod, Protection des données médicales et transparence… du patient ? Berne 2012, p. 56.

97 Sabrina Burgat, Carte d'assuré dossier patient informatisé, E-health : récents développements, in : Olivier Guillod, Protection des données médicales et transparence… du patient ? Berne 2012, p. 60.

98 Conseil fédéral, Message concernant la loi fédérale sur le dossier électronique du patient (LDEP) du 16 septembre 2011, p. 11 ; Agnès Hertig Pea, La protection des données personnelles médicales est-elle efficace ? Etude des moyens d'action en droit suisse, Neuchâtel 2013, p. 79, N. 210.

commandations en matière de normes et d'architecture de la stratégie e-Health[99].

Le PFPDT invité à se prononcer sur la stratégie « Cybersanté Suisse » du Conseil fédéral a émis des doutes y relativement, dès mai 2013, en indiquant être inquiet parce que cette stratégie vise à favoriser l'échange de données du patient[100]. De son point de vue, cette stratégie n'était pas encore clairement définie. Qui seront les personnes autorisées à consulter le dossier électronique d'un patient? Selon quels critères? Qu'advient-il de ces données une fois le traitement médical achevé? Les questions sont multiples et les réponses nébuleuses. La réponse la plus intéressante formulée dans ce contexte a trait à la possibilité pour chaque canton de mettre cette stratégie sur pied comme il l'entend : « *C'est problématique et cela compliquera davantage la protection de la sphère privée des patients* ». Le PFPDT avait parfaitement appréhendé les risques inhérents aux choix législatifs opérés.

La loi sur le dossier électronique du patient du 19 juin 2015 (abrégée ci-après LDEP) entrera très probablement en vigueur durant l'été 2017. Celle-ci prévoit à son article 12 intitulé « *critères de certification* » que le Conseil fédéral fixe les critères de certification en tenant compte des normes internationales en la matière et des progrès techniques, en particulier en ce qui concerne:

a. les normes, les standards et les profils d'intégration applicables;
b. la garantie de la protection et de la sécurité des données;
c. les prescriptions organisationnelles.

L'Office fédéral de la santé publique (OFSP) peut être habilité[101] à adapter aux progrès techniques les critères visés à l'article 12 al. 1 LDEP. Ces dispositions

---

99 e-Health Suisse, Normes et architecture Recommandations IIII, identification de personnes et système d'autorisation, adoptées par le comité de pilotage, Berne, le 23 octobre 2011. Les normes et architectures sont consultables sur ce site : <http://www.e-health-suisse.ch/umsetzung/00146/00148/index.html?lang=fr>.

100 Le Temps du 5 mail 2013 : <http://www.letemps.ch/suisse/2013/05/05/on-ne-mesure-impact-big-data-sphere-privee>.

101 Article 12 al. 2 LDEP.

légales peuvent être qualifiées d'exsangues en termes de protection et de sécurité des données et elles nécessitent une concrétisation qui est actuellement en cours. Au vu du type de données et de l'intérêt représenté pour les hackers par une base de données de ce type, il conviendrait *a minima* d'exiger que toutes les données soient cryptées. Il eût été possible de renvoyer en cette matière éminemment technique et complexe, s'agissant de la garantie de la protection et de la sécurité des données, à la LPD et son ordonnance d'application. Cela aurait évité que les personnes et entités intéressées à ce type de projets ne doivent débattre relativement à la portée des normes internationales et aux progrès techniques. De plus, on perçoit mal comment le Conseil fédéral, avec la charge de travail qui est la sienne, pourra adapter de manière constante les standards de sécurité. Quoi qu'il en soit la responsabilité en cas de perte ou de vol de données, dans l'hypothèse où les standards les plus restrictifs devaient ne pas être adoptés et que de ce fait les données devaient être diffusées, lui incombera exclusivement. Il est même possible d'imaginer des procédures pénales, dans l'hypothèse où de graves manquements devaient être constatés et documentés. C'est un choix singulier que celui-ci et le soussigné doute que le Conseil fédéral soit pleinement conscient de toutes les conséquences qui en résulteront.

Avant l'entrée en vigueur de la LDEP, deux cantons soit le Valais[102] et Genève[103] ont décidé d'introduire, de manière distincte, le dossier électronique du patient[104]. À la différence du système « INFOMED » mis en œuvre par le Canton du Valais, il n'y a pas de dossier centralisé sur la plateforme MDM genevoise, les données médicales demeurant dans les locaux des organisations médicales sur les serveurs secondaires, de sorte qu'on ne peut pas, à proprement parler techniquement de dossier électronique du patient, mais plutôt d'un système de partage de documents médicaux informatisés. Ce choix d'architecture informatique a manifestement un impact sur la sécurité

102 Le projet s'intitule INFOMED, cf. <www.infomed-vs.ch>.

103 Le projet s'intitule Mon Dossier Médical (MDM), cf. <http://www.mondossiermedical.ch>.

104 Pour un état des lieux au 4 décembre 2015 : <http://www.tdg.ch/suisse/Le-dossier-electronique-du-patient-se-concretise/story/24453308>.

des données et il est de ce point de vue singulier que des choix aussi diamétralement opposés soient possibles, alors qu'une démarche d'uniformisation au niveau fédéral a tout son sens, entre autres pour accroître le niveau de sécurité et de maturité des systèmes d'information.

Sur le plan législatif, contrairement au choix opéré par le Canton de Genève[105], le Canton du Valais a singulièrement adopté une ordonnance concernant le système d'échange d'information sanitaire (Ordonnance « Infomed », abrégée ci-après OInfomed[106]) du 18 septembre 2013 (RS 800.001). Cette démarche prête manifestement à discussion.

La communication de données est régie dans le Canton du Valais par les articles 22 et suivants de la Loi sur l'information du public, la protection des données et l'archivage (LIPDA) du 9 octobre 2008[107]. Selon l'article 22 alinéa 2 de la LIPDA :

Les données sensibles peuvent être communiquées à des tiers par les autorités lorsqu'une des trois conditions suivantes est remplie:

a. une disposition contenue dans une loi au sens formel les y autorise;

b. la personne concernée y a, en l'espèce, consenti expressément;

c. la communication est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'une tierce personne.

Cet alinéa traite de l'accès à des données sensibles qui doit être réglé de manière plus stricte. Leur communication ne peut avoir lieu que si elle est prévue dans une loi au sens formel. Contrairement à l'alinéa 1, une disposition légale quelconque (par exemple dans une ordonnance) ne suffit pas. Alternativement, la communication peut avoir lieu si la personne concernée y a, en l'espèce, consenti expressément. Un consentement résultant de l'ensemble

105 Le Canton de Genève a adopté le 14 novembre 2008 la loi sur le réseau communautaire d'informatique médicale (e-Toile)(LRCIM), accessible à cette adresse <http://160.53.186.12/legislation/rsg/f/s/rsg_K3_07.html>.

106 Il s'agit d'une abréviation choisie par le soussigné.

107 Cette loi trouve application notamment en vertu de la teneur de l'article 17 OInfomed.

des circonstances n'est pas non plus suffisant. Finalement, les autorités peuvent transmettre des données sensibles si la communication est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'une tierce personne. Le but principal de cette disposition est d'éviter que n'importe quel intérêt public ou privé puisse suffire à autoriser la communication des données sensibles à des tiers.

Les données personnelles ainsi que les données sensibles peuvent, dans des cas concrets, être transmises aux autorités et organes publics qui en font la demande si la transmission est autorisée par la loi ou si les informations sollicitées sont nécessaires à l'accomplissement de leurs tâches (article 22 al. 3 LIPDA).

Il existe des situations où le consentement ne pourra pas être recueilli, ce qui signifie qu'une base légale formelle doit alors exister pour permettre la communication de données. À titre exemplatif, l'article 12 alinéa 1er OInfomed prévoit, dans les situations d'urgence, la possibilité pour tout professionnel de la santé ou établissement ou institution sanitaire participant au système d'échange d'information d'accéder aux données relatives à un patient déterminé si la vie ou la santé de ce patient est menacée d'un danger imminent, à moins que le patient ou son représentant l'ait exclu préalablement. Une telle communication fondée sur une ordonnance en l'absence du consentement est contraire à l'article 22 alinéa 2 LIPDA. Concrètement, cela signifie donc que cet article est, dans les faits, inapplicable.

Rappelons à cet égard que le Tribunal fédéral a admis explicitement que les dossiers médicaux qui, par nature, contiennent des informations très personnelles et intimes bénéficient de la protection des droits fondamentaux[108]. Nonobstant le fait que la Constitution fédérale ne comporte pas mention des catégories de données sensibles du droit fédéral et cantonal, à l'aune de l'article 36 Cst. des exigences constitutionnelles plus strictes doivent être

108 ATF 122 I 153, p. 163, consid. 6 b) bb).

respectées pour justifier les atteintes à des droits fondamentaux dues au traitement de données relatives à la santé[109].

De telles exigences ne sauraient être respectées par l'édiction et l'adoption d'une simple ordonnance, qui ne constitue pas une base légale formelle. Il y a donc, en l'occurrence, violation de l'article 36 de la Constitution fédérale, car nous nous trouvons en présence de restrictions graves des droits fondamentaux (cf. à titre exemplatif l'article 12 OInfomed). Ainsi qu'il a été exposé, les dossiers médicaux comportent intrinsèquement des données sensibles. Il n'est dès lors pas envisageable de prévoir des restrictions sur la base d'une simple ordonnance. Le traitement la récolte et la conservation de données personnelles sensibles sont effet considérés comme une restriction grave[110] et ils nécessitent une réglementation claire et expresse contenue dans une loi au sens formel[111]. Il est, de ce point vue, étonnant que cette problématique ait échappé à un examen attentif, qui génère aujourd'hui la nécessité d'une interruption de tout traitement de données, dans l'attente de l'adoption d'une base légale formelle.

En bref, le principe de densité normative en matière de protection des données n'est pas respecté par l'édiction et l'adoption d'une ordonnance, de surcroît exsangue sur des points fondamentaux tels que le droit à l'autodétermination informationnelle[112].

---

109 Cf. l'avis de droit émis le 12 décembre 2014 par le Professeur Andreas Glaser, intitulé « Avis de droit succinct sur des questions concernant le consentement et la présomption de consentement ainsi que la participation d'institutions de droit public à une communauté dans le contexte du projet de loi sur le dossier électronique du patient, p. 5, §II/1 et les références citées, avis de droit disponible à cette adresse : <http://www.e-health-suisse.ch/umsetzung/00282/index.html?lang=fr>.

110 ATF 122 I 360.

111 Aline Schmidt Noël, La limitation des droits fondamentaux en droit constitutionnel comparé, Neuchâtel, p. 48 et les nombreuses références citées.

112 Cf. également l'avis de droit émis le 12 décembre 2014 par le Professeur Andreas Glaser, intitulé « Avis de droit succinct sur des questions concernant le consentement et la présomption de consentement ainsi que la participation d'institutions de droit public à une communauté dans le contexte du projet de loi sur le dossier électronique du patient, p. 4, §II/1, disponible à cette adresse : <http://www.e-health-suisse.ch/umsetzung/00282/index.html?lang=fr>.

Cette ordonnance, comportant 21 articles, évoque la sécurité et la sécurisation des données en 10 articles en ces termes :

Section 4 : Accès aux données

Art. 11 Identification et authentification du patient et des professionnels de la santé
[1] L'accès aux données par le patient et par les professionnels de la santé est authentifié par un double facteur («authentification forte»).
[2] L'accès aux données par les professionnels de la santé peut s'effectuer au moyen de la carte délivrée par leur association professionnelle si elle comporte un moyen d'identification personnelle.

Art. 12 Situations d'urgence
[1] Tout professionnel de la santé ou établissement ou institution sanitaire participant au système d'échange d'information peut accéder aux données relatives à un patient déterminé si la vie ou la santé de ce patient est menacée d'un danger imminent, à moins que le patient ou son représentant l'ait exclu préalablement.
[2] Un tel accès est signalé au patient ou à son représentant.

Section 5: Droits reconnus au patient

Art. 13 Accès aux données qui le concernent
[1] Le patient peut accéder aux données le concernant qui sont traitées par le système d'échange d'information.
[2] Le patient peut saisir lui-même certaines données le concernant.

Art. 14 Droit du patient à définir les destinataires et les niveaux d'accès des destinataires
[1] Le patient peut définir les professionnels de la santé et les établissements et institutions sanitaires qui ont accès aux données le concernant.
[2] Le patient peut limiter les droits d'accès des professionnels de la santé ou établissements et institutions sanitaires à certaines données le concernant.
[3] Le patient peut modifier en tout temps les droits d'accès et les niveaux d'accès qu'il a définis.

Art. 15 Liste des accès

[1] Le patient peut en tout temps obtenir la liste des professionnels de la santé et établissements et institutions sanitaires ayant accès ou ayant eu accès aux informations le concernant.

[2] Les historiques doivent être conservés pendant dix ans.

Art. 16 Rectification de données inexactes ou incomplètes

Le patient peut demander que toute donnée inexacte ou incomplète le concernant soit rectifiée.

Section 6: Protection des données

Art. 17 Confidentialité des données

[1] Les données récoltées sont traitées confidentiellement, dans le respect des normes imposant le secret professionnel ou le secret de fonction et de la législation sur la protection des données.

[2] Le comité de direction dans la phase de développement puis l'organisme responsable du système d'échange d'information dans la phase d'exploitation collaborent avec l'autorité cantonale chargée de la protection des données pour assurer le respect des normes en vigueur.

Art. 18 Utilisation des données à des fins statistiques

L'utilisation à des fins statistiques de données anonymes ne permettant pas d'identifier les patients concernés est autorisée.

Art. 19 Mesures organisationnelles et techniques

[1] Des mesures appropriées sont prises pour la protection des données enregistrées contre les risques de falsifications, de destruction, de vol, de perte, de copies et autres traitements illicites.

[2] Ces mesures doivent notamment permettre la traçabilité du traitement (création, modification et accès) des données enregistrées au sein du système d'échange d'information.

L'Ordonnance prévoit des sanctions en ces termes :

Section 7: Sanctions

Art. 20 Renvoi à la législation fédérale et cantonale
Les professionnels de la santé et les organes des établissements et institutions sanitaires qui contreviendraient aux dispositions du droit fédéral et du droit cantonal concernant le dossier électronique du patient, la protection des données, le devoir de confidentialité imposé aux professionnels de la santé et les droits des patients sont passibles des sanctions prévues par ces législations.

À la lecture de ces différentes normes, l'on constate immédiatement que si celles-ci sont plus exhaustives et précises que ne le sont celles qui sont contenues dans la LDEP, il n'en demeure pas moins que les exigences en termes de protection des données et de sécurité ne sont pas spécifiées. Dans ces circonstances, il existe un risque d'appréhension différenciée par les cantons du fait de l'absence de concrétisation des attentes et exigences liées à l'application de l'article 12 LDEP[113], respectivement à l'article qui a précédé. Une telle situation est déconcertante, en tant qu'elle consiste à ne pas fixer de cadre légal fédéral suffisamment précis et à laisser les Cantons implémenter des systèmes sur la base de normes qu'ils se sont donnés. À titre exemplatif, cela équivaudrait à mettre en service une autoroute, sans définir le sens de circulation, la limitation de vitesse et les véhicules autorisés à l'emprunter. Ce manque d'anticipation, associé au fait qu'eHealth Suisse n'a opéré aucune vérification relative à la sécurité des systèmes d'information ont créé une situation qui s'apparente à une mise en danger de données sensibles. Le fait qu'il s'agisse d'une loi-cadre n'excuse en rien des défauts aussi saillants.

Dans de telles circonstances et un contexte législatif aussi squelettique, les interrogations sont plus nombreuses que les bonnes pratiques :

113 L'OInfomed se réfère expressément dans son préambule au projet de loi fédérale sur le dossier électronique du patient du 29 mai 2013 (LDEIP), ce qui signifie que le contenu du projet a été intégré au texte d'OInfomed.

- La déclaration de fichiers[114] qui revêt une grande importance pour assurer le respect de la loi[115] doit-elle être formulée chez le Préposé fédéral et/ou les Préposé(e)s des différents cantons ?
- Quelles doivent être les qualifications des collaborateurs qui officient pour assurer la sécurité de systèmes d'informations aussi sensibles ?
- Doivent-ils être certifiés[116] ?
- Respectivement le SMSI doit-il être certifiés ISO 27001 et/ou ISO 29100 ?
- Les données doivent-elles être cryptées ?
- À quelle fréquence les audits de sécurité doivent-ils être réalisés ?
- Un audit organisationnel ISO 27001 : 2013 est-il obligatoire ?
- Est-il autorisé de confier un mandat de prestation à une société étrangère si son siège se trouve dans l'UE ?
- Dans cette hypothèse, quelles démarches doivent être entreprises pour s'assurer du respect des normes légales suite à cette délégation du traitement de données ?
- Comment obtenir la restitution des données en possession du prestataire en cas de rupture du contrat ?
- Que se passe-t-il en cas de faillite, respectivement comment prévenir et éviter le fait que les données ne tombent dans la masse en lite[117] ?

---

114 Les fichiers sensibles doivent être déclarés tant au Préposé fédéral qu'aux Préposé(e)s des différents cantons en vertu de l'article 11a alinéa 3 LPD et des dispositions topiques cantonales.

115 Comment vérifier les fichiers dont on ignore jusqu'à l'existence ? Les Préposé(e)s ont souvent recours à un catalogage pour informer et diligenter les vérifications, mais la règle légale qui prévaut est bien l'obligation d'annonce préalable au traitement.

116 Par exemple, Information Security Lead Auditor ISO 27001 :2013, Security Management Lead Implementer ISO 27001 :2013 ou encore Certified Lead Privacy Implementer ISO 29100.

– Etc.

Il est certain pour le soussigné, après avoir passé plus de 5 mois à auditer Infomed, que différentes démarches sont absolument nécessaires pour assurer la sécurité des données et établir la confiance nécessaire dans un domaine où le succès d'une telle démarche si dépendant d'elle :

– Les audits de sécurité devraient être ordonnés et réalisés par une structure externe et fédérale aux fins de permettre un processus de sélection des meilleurs experts (qui seraient accrédités) et d'éviter la tendance naturelle à se montrer moins incisif avec celui qui vous rémunère.

– Ces audits devraient s'avérer imprévisibles comme en matière de dopage, de sorte que leur fréquence, leur ampleur et nature ne seraient pas connus et feraient l'objet de changements réguliers.

– Les résultats de différents audits réalisés devraient servir à améliorer le processus métier et à affiner les exigences légales sur une base tant scientifique que pragmatique.

– Aucune donnée médicale ne devrait jamais être transmise à l'étranger ni sauvegardée dans un pays étranger, ne serait-ce que parce qu'il est impossible d'éviter les accès de tierces parties (gouvernements notamment), la vente de ces données et la concrétisation des risques liés à une faillite de la société prestataire.

---

117 Le PFPDT évoque dans son rapport annuel 2014/2015 le cas de la vente de données d'un cabinet de médecin dentiste, un Office des faillites ayant considéré que de telles données avaient une valeur marchande et pouvaient faire l'objet d'une vente forcée. Après avoir été consulté bien que la compétence soit cantonale, le PFPDT a émis l'avis suivant : « *un office des faillites ne peut vendre des données de patients à un successeur prêt à racheter le cabinet sans avoir préalablement consulté les patients. L'accord des patients constitue une condition indispensable à la transmission des données à l'acquéreur du cabinet* », 22ème Rapport d'activité 2014/2015 du PFPDT, p. 41 ; le rapport est accessible ici : <http://www.edoeb.admin.ch/dokumentation/00153/01251/index.html?lang=fr>.

- L'autorité de surveillance cantonale devrait être totalement indépendante des personnes qui intègrent un comité de pilotage ou de direction de manière à respecter le principe des quatre yeux[118].
- De manière générale, en cas de problème d'importance, une structure fédérale (OFSP ou eHealth Suisse ?) devrait pouvoir immédiatement intervenir dans le respect du fédéralisme pour empêcher toute atteinte irréversible aux droits de patients notamment.
- Le cryptage des données devrait être la règle.
- Etc.

Ces différents éléments font actuellement l'objet d'un examen dans le cadre de l'élaboration de la future ordonnance sur le dossier électronique du patient. Il paraît à cet égard pertinent que les cantons ayant déjà introduit un tel dossier soient associés aux démarches de mise en place du privacy and security shield qui doit assurer aux utilisateurs un niveau très élevé de protection. Cette ordonnance doit de surcroît viser l'excellence en termes de normes de sécurité, car à l'aune des développements dans le domaine informatique, ce qui est sûr aujourd'hui ne le sera plus dans un an et même probablement plus dans quelques mois. Les normes doivent donc être rédigées de manière neutre afin de permettre une adaptation rapide exempte de la nécessité d'un processus législatif par nature lent et complexe[119].

---

118 Le principe des quatre yeux est un instrument de gestion, de développement et de controlling de la qualité employé par beaucoup d'organisations. Il désigne le fait que quatre yeux (donc deux personnes) peuvent voir davantage de choses que deux yeux, à la fois au niveau de ce qui est (réalité) et de ce qui pourrait être (possibilités) et diligenter des vérifications plus efficaces.

119 Sébastien Fanti, Le dossier patient, Graal de l'économicité ou forteresse digitale, in : Revue de la société vaudoise de médecine, novembre 2015, p. 7.

3.3 Les objets connectés – privacy by design & privacy by default – privacy shield

On parle d'objets connectés pour définir des types d'objets dont la vocation première n'est pas d'être des périphériques informatiques ni des interfaces d'accès au web, mais auxquels l'ajout d'une connexion Internet a permis d'apporter une valeur supplémentaire en termes de fonctionnalité, d'information, d'interaction avec l'environnement ou d'usage[120].

Une récente étude[121] publiée en février 2016 et conduite en partenariat entre le *Citizen Lab* de l'Université de Toronto et Open Effect[122] portant sur huit appareils connectés[123] a démontré que les traqueurs d'activité ne respectaient pas les normes de confidentialité[124] :

Most devices we studied do not implement Bluetooth privacy and this leaves users vulnerable to location-based surveillance. We hope our findings will help consumers make more informed decisions about how they use fitness trackers, help companies improve

120 Il s'agit de la définition du Dictionnaire du Web : <http://www.dictionnaireduweb.com/objet-connecte/>.

121 L'Étude qui s'intitule : « *Every Step You Fake: À Comparative Analysis of Fitness Tracker Privacy and Security* est disponible à cette adresse : <https://openeffect.ca/reports/Every_Step_You_Fake.pdf>.

122 Open Effect is a Canadian not-for-profit applied research organization focusing on digital privacy and security.

123 Apple Watch, Basis Peak, Fitbit Charge HR, Garmin Vivosmart, Jawbone Up 2, Mio Fuse, Withings Pulse O2, et Xaomi Mi Band.

124 Il ne s'agit, en réalité, pas d'une surprise, car des spécialistes en sécurité avaient mis en exergue des problèmes d'implémentation liés au protocole Bluetooth Low Energy par le passé ; les objets connectés émettent en permanence des paquets intégrant une adresse MAC pour signaler leur présence et inviter à se connecter ; pour éviter la surveillance, le protocole BLE a été doté d'un mécanisme baptisé « *LE Privacy* » qui change de manière aléatoire l'adresse qui est broadcastée ; cette fonction est mal implémentée : pour la plupart des objets testés, l'adresse reste fixe ; dans d'autres cas, c'est pire : les adresses des fabricants Nike ou MI, par exemple, commencent toutes de la même manière, ce qui rend l'identification des appareils aisée, source : Gilbert Kallenborn, Espionner les objets connectés, c'est facile grâce au Bluetooth LE, article publié le 27 mai 2015 sur le site 01net.com : <http://www.01net.com/actualites/espionner-les-objets-connectes-c-est-facile-grace-au-bluetooth-le-655726.html>.

the privacy and security of their offerings, and help regulators understand the current landscape of wearable products." — Andrew Hilts, Executive Director, Open Effect and Research Fellow, The Citizen Lab, Munk School of Global Affairs, and the University of Toronto[125].

Parmi les modèles testés, seule l'Apple Watch utiliserait une adresse MAC aléatoire. Sans la protection apportée par ce système, ses personnes mal intentionnées peuvent aisément accéder aux informations telles que les données de santé des utilisateurs, voire même les modifier. Il serait également possible de géolocaliser les utilisateurs de ces sept produits, et ce même si le bracelet n'est pas jumelé avec votre téléphone[126] !

Cette étude démontre, une nouvelle fois, que sécurité, respectivement la protection des données doit être abordée *ab initio*. Le droit suisse ne connaît pas[127] encore le principe de « *privacy by design*[128] », qui vise à intégrer des mesures protégeant les données personnelles, dès la conception. Le *privacy by design*[129] vise la prévention en matière d'atteinte à la vie privée, plutôt que la réaction suite à une atteinte[130]. Le principe du *privacy by default*[131] signifie

125 <https://citizenlab.org/2016/02/security-privacy-issues-several-leading-wearable-fitness-tracking-devices/>.

126 Dave Calpito, Most Fitness Trackers Except The Apple Watch Are Leaking Your Private Information: Study, Tech Times, 3 février 2016 : « *The study notes that all of these devices, with the exception of the Apple's smart timepiece, make it possible for hackers to trace the owners by means of Bluetooth, even when they are not paired with a smartphone. It explains that each of these wearables makes use of a Bluetooth technology emitting a signal plus a unique identifier that can be tracked. The researchers conclude that this can leave users subjected to long-term tracking of their location.* » ; <http://www.techtimes.com/articles/130186/20160203/most-fitness-trackers-except-the-apple-watch-are-leaking-your-private-information-study.htm>.

127 Contrairement notamment à nos voisins européens, cf. directive 95/46/CE.

128 En français PIVP, soit Protection Intégrée de la Vie Privée.

129 Cf. également Michel Jaccard, De la protection des données à la sécurisation des données connectées ?, in : Regards de marathoniens sur le droit suisse, Mélanges publiés à l'occasion du 20ème « Marathon du droit », Genève 2015, p. 500 et les références citées.

130 Agnès Hertig Pea, La protection des données médicales est-elle efficace ?, Neuchâtel 2013, p. 299.

quant à lui que les réglages par défaut doivent préserver au maximum la sphère privée. Ces deux concepts ont fait l'objet d'interventions parlementaires de la part du Conseiller national Jean-Christophe Schwaab[132] et du Conseiller aux États Luc Recordon[133], toutes couronnées de succès, puisque le Conseil fédéral a proposé d'accepter les postulats.

Le groupe d'accompagnement révision LPD a examiné, au titre des mesures de diligence, l'introduction lors de la prochaine révision de la loi[134] des principes de *privacy by design* et *privacy by default* et s'est exprimé en ces termes[135] :

– Principe du « Privacy by Design »: obligation pour les responsables du traitement de données (ou de leurs éventuels sous-traitants), dès la conception du traitement – pour autant qu'il porte sur des données personnelles – de tenir compte des exigences en matière de protection des données et de prévoir des mesures de protection adéquates (p. ex : limitation au strict minimum des données traitées par l'application; sauvegarde décentralisée des données personnelles obtenues; intégration de mesures de sécurité techniques permettant de réduire le risque de traitements illicites des données). Pour l'application de cette obligation, il convient de prendre en considération notamment les risques que le traitement de données prévu présente pour la protection de la personnalité, les possibilités tech-

131 Cf. également Michel Jaccard, De la protection des données à la sécurisation des données connectées ?, in : Regards de marathoniens sur le droit suisse, Mélanges publiés à l'occasion du 20ème « Marathon du droit », Genève 2015, p. 501 et les références citées.

132 Postulats Schwaab 13.3806 « La protection de la sphère privée doit être garantie par défaut » et 13.3807 « Un renforcement de la protection des données grâce au « privacy by design », tous deux acceptés par le Conseil fédéral.

133 Postulat Recordon 13.3989 « Violations de la personnalité dues au progrès des techniques de l'information et de la communication », accepté par le Conseil fédéral.

134 Rapport du groupe d'accompagnement Révision LPD « *Esquisse d'acte normatif relative à la révision de la loi sur la protection des données* » du 29 octobre 2014, p. 17 à 20.

135 Rapport du groupe d'accompagnement Révision LPD « Esquisse d'acte normatif relative à la révision de la loi sur la protection des données » du 29 octobre 2014, p. 17 à 18.

niques, les standards reconnus ainsi que les coûts liés aux mesures. Dans ce cadre, on portera une attention particulière aux besoins de protection des mineurs et d'autres groupes de personnes particulièrement vulnérables.

– Principe du « Privacy by Default »: si les utilisateurs d'une application traitant des données ont la possibilité de choisir entre différents paramétrages, le réglage par défaut sera celui qui assure la plus grande protection des données personnelles. Il convient de tenir compte tout spécialement du besoin de protection des mineurs et d'autres groupes de personnes particulièrement vulnérables.

Nous saurons d'ici à quelque mois, dans le cadre de la présentation de l'avant-projet[136], quelles normes seront proposées en vue d'intégrer ces principes à notre législation. D'ici là le consommateur devra être très attentif lorsqu'il opte pour un objet connecté et configurer correctement ce qui s'apparente à des aspirateurs de données, voire à des espions[137]. Les délices et les espoirs générés par le quantified self[138] ne doivent pas occulter les risques en termes de sécurité des systèmes d'informations et de profiling[139].

---

136 Cf. § 2.2.

137 Confer à cet égard le reportage diffusé par Arte le 29 octobre 2015 intitulé « Objet connectés, des espions parmi nous ? », <http://future.arte.tv/fr/objets-connectes-ce-quils-disent-de-vous/les-objets-connectes-des-espions-parmi-nous>.

138 Il s'agit d'un mouvement qui regroupe les outils, les principes et les méthodes permettant à chacun de mesurer ses données personnelles, de les analyser et de les partager2. Les outils du quantified self peuvent être des objets connectés, des applications mobiles ou des applications Web ; <https://fr.wikipedia.org/wiki/Quantified_self>.

139 Sébastien Fanti, Utopies.2016, Blog Lawdrag@on, Digital Law Clinic: l'univers numérique passé au scanner, 2 janvier 2016: Dans un monde où la faiblesse sous toutes ses formes est honnie, nous générons par notre partage d'informations, souvent anodines, un véritable profiling de santé, dont les montres connectées sont les aspirateurs de données. Le danger est immense d'en subir les conséquences à brève échéance: **un suicide numérique**. Démonstration par l'exemple, avec votre Serviteur! Les seules publications sur les réseaux sociaux permettront à tout assureur maladie de personnifier les nuits courtes, les interruptions de cycles de sommeil, le coucher à heures irrégulières. En bref Morphée n'est guère mon amie. Quant aux images diffusées sur Instagram, elles renseigneront sur la nature et la qualité des plats, les habitudes alimentaires et seront susceptibles d'effrayer le plus aguerri des réassureurs. En bref,

Dans la mesure où la majorité des acteurs du marché des objets connectés se trouve aux USA se pose désormais légitimement la question de la légalité du transfert des données dans ce pays.

Depuis janvier 2009, le « U.S.-Swiss Safe Harbor Framework » constituait un instrument visant à garantir un niveau de protection suffisant pour les données transférées vers les États-Unis[140]. L'envoi par les objets connectés de données vers les USA était donc susceptible de respecter les conditions évoquées par le Préposé fédéral[141]. L'arrêt relatif à l'accord « Safe Harbor » rendu le 6 octobre 2015 (affaire C-362/14, *Schrems*[142]) par la Cour de justice de l'Union européenne (CJUE) a invalidé l'accord de protection des données « Safe Harbor » conclu entre l'Europe et les États-Unis. La Cour a en effet constaté que le transfert de données personnelles vers ce pays sous la forme prévue par l'accord était problématique. Selon le Préposé fédéral à la protection des données et à la transparence, cela signifie ceci pour la Suisse[143] :

« *Tant que la Suisse n'a pas renégocié un nouvel accord avec le gouvernement américain, l'accord « U.S.-Swiss Safe Harbor Framework » ne constitue plus une base légale suffisante pour une transmission de données personnelles aux États-Unis compatible avec la loi suisse sur la protection des données (LPD). Dans l'intervalle, le PFPDT recommande, pour l'échange de données personnelles avec des entreprises américaines, de convenir de garanties contractuelles au sens de l'art. 6, al. 2, let. a, LPD. Même si ces garanties ne règlent pas le problème d'accès disproportionnés des autorités, elles permettent d'améliorer le niveau de protection des données.*

---

je ténorise les risques, comme d'autres collectionnent les timbres. À leur place, je ne m'assurerais pour rien au monde.

140 Pour de plus amples informations, cf. <http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/index.html?lang=fr>.

141 <http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr>.

142 L'arrêt est accessible à cette adresse : <http://curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FR&cid=384796>.

143 <http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr>.

Il convient de mettre en œuvre les mesures suivantes:

- Les personnes dont les données sont transmises aux États-Unis doivent être informées de manière claire et aussi exhaustive que possible des accès possibles des autorités, afin de leur permettre d'exercer leurs droits. Le contrat d'échange de données personnelles devrait prévoir un engagement des parties contractantes dans ce sens.
- Les parties doivent s'engager à mettre à la disposition des personnes concernées les outils nécessaires à une protection juridique efficace, à exécuter réellement les procédures correspondantes et à accepter les décisions qui en résultent ».

Le Préposé fédéral a sollicité des entreprises helvétiques qu'elles procèdent aux adaptations contractuelles requises jusqu'à la fin janvier 2016. À l'instar des autres autorités européennes, il pourrait prendre d'autres mesures à l'échéance de ce délai pour faire respecter la loi. Il paraît également important de mettre en exergue le fait que toute personne concernée par un traitement de données peut à tout moment faire examiner par un tribunal civil les données devant être transmises aux États-Unis[144].

Il a émis un rapport et différentes recommandations, datés du 14 octobre 2015, à l'intention du Conseil fédéral dont voici le libellé :

a. *Il conviendrait de décider de résilier l'accord « U.S.-Swiss Safe Harbor Framework » conclu avec les États-Unis d'Amérique en 2008 et de le remplacer par un nouvel accord satisfaisant aux exigences de la loi fédérale sur la protection des données (LPD, RS 235.1), ou par une autre solution remplissant également ces exigences.*
b. *Il conviendrait subsidiairement de décider de suspendre l'accord « U.S.-Swiss Safe Harbor Framework » conclu avec les États-Unis d'Amérique en 2008 jusqu'à ce que de nouvelles négociations aient permis de parvenir à la satisfaction des exigences posées par la loi fédérale sur la protection des données (LPD,*

144 Cf. notamment RVJ 2015 259.

RS 235.1), ou qu'une autre solution soit trouvée et mise en œuvre, qui remplisse également ces exigences.

c. *Les départements compétents devraient être chargés de mettre en œuvre cette décision et d'informer les autorités américaines en conséquence.*

d. *La Mission de la Suisse auprès de l'Union européenne à Bruxelles devrait être mandatée pour prendre contact avec la Commission européenne afin de coordonner la suite de la procédure.*

À la connaissance du soussigné, le Conseil fédéral n'a pas encore pris de décision suite à ces recommandations.

Depuis, l'Union européenne et les États-Unis ont annoncé le 2 février 2016 un accord relatif à un Privacy Shield[145] successeur du Safe Harbor, soit un bouclier censé protéger les données, lors de leur transfert. Voici quelques exemples de dispositifs prévus par le Privacy Shield[146] :

- des garanties écrites et détaillées apportées par les États-Unis afin d'assurer que l'accès aux données des citoyens européens par les autorités publiques à des fins de sécurité nationale sera limité et contrôlé ;
- des engagements pris par les entreprises importatrices des données de respecter des obligations rigoureuses sur le traitement des données et le respect des droits des personnes concernées, sous la surveillance du « Department of Commerce » ;
- la définition de plusieurs voies de recours pour les citoyens européens tant en Europe qu'aux États-Unis avec notamment une voie d'arbitrage possible en dernier recours ;

145 Bouclier de protection de la privacité.

146 Annabelle Richard et Anne-Sophie Mouren, Du Safe Harbor au « Privacy Shield » : de réels progrès ou « blanc bonnet, bonnet blanc » ?, article publié le 3 février 2016 sur le site ZDNet.fr : <http://www.zdnet.fr/actualites/du-safe-harbor-au-privacy-shield-de-reels-progres-ou-blanc-bonnet-bonnet-blanc-39832094.htm>.

- une clause de révision annuelle permettant de surveiller de près que ce dispositif est correctement mis en place ;
- des sanctions voire l'exclusion des entreprises importatrices de données du nouveau dispositif pourraient être appliquées à l'encontre des entreprises se trouvant en violation de leurs obligations ;
- etc.

Les interrogations relatives à cet accord sont nombreuses et protéiformes : ce Privacy Shield est-il un bouclier de papier[147] respectivement un accord aussi peu efficient que le précédent[148] ? Des motifs plurifactoriels incitent à la plus grande prudence. Ainsi que le met en exergue François Charlet, dans un article récent consacré à cette thématique[149], il est urgent d'attendre, car les autorités en matière de protection des données n'ont pas encore pu prendre connaissance de l'ensemble des documents qui concrétisent et composent l'accord. Un délai à la fin février 2016 a été octroyé à la Commission européenne pour obtenir ces informations[150] : *« Il l'examinera à la lumière de ces garanties essentielles et évaluera s'il répond aux préoccupations importantes relatives aux transferts internationaux de données soulevées par la décision de la CJUE. Le G29[151] se réunira en séance plénière dans les semaines suivantes et rendra publique son analyse au mois d'avril »*. Rien ne garantit donc que ce Privacy Shield sera considéré comme un outil assurant un niveau de protec-

147 Marc Rees, Après le Safe Harbor, le Privacy Shield. Un bouclier de papier ?, article publié sur le site nextimpact le 3 février 2016 : <http://www.nextinpact.com/news/98366-apres-safe-harbor-privacy-shield-un-bouclier-papier.htm>.

148 Annabelle Richard et Anne-Sophie Mouren, Du Safe Harbor au « Privacy Shield » : de réels progrès ou « blanc bonnet, bonnet blanc » ?, article publié le 3 février 2016 sur le site ZDNet.fr : <http://www.zdnet.fr/actualites/du-safe-harbor-au-privacy-shield-de-reels-progres-ou-blanc-bonnet-bonnet-blanc-39832094.htm>.

149 François Charlet, EU-US Privacy Shield : une grande farce ?, article publié le 8 février 2016, disponible ici : <https://francoischarlet.ch/2016/eu-us-privacy-shield-une-grande-farce/>.

150 Cf. à cet égard, <http://www.cnil.fr/linstitution/actualite/article/article/safe-harbor-le-g29-analyse-les-consequences-de-la-decision-de-la-cjue/>.

151 Il s'agit du groupe des autorités en matière de protection des données européennes, cf. <https://fr.wikipedia.org/wiki/G29>.

tion adéquat s'agissant du transfert des données entre l'Europe et les États-Unis et il est même d'en douter très sérieusement du seul fait que pour la protection des citoyens soit effective, des lois américaines doivent être amendées.

Dans un article récent du Point[152], l'intérêt des services de renseignement pour les objets connectés a été mis en exergue. Il y est notamment relaté la mort suspecte d'un génial hacker Barnaby Jack[153], qui était capable de prendre le contrôle d'un pacemaker ou d'une pompe à insuline, donc de tuer à distance. Il avait ainsi mis au jour les vulnérabilités des dispositifs médicaux embarqués[154]. Il n'est pas fantaisiste d'imaginer que l'on prenne la main, demain, sur votre thermostat ou sur l'ouverture de votre porte – une start-up, Lockitron, a produit son premier modèle de serrure connectée –, tout comme il n'est pas fantaisiste d'imaginer l'incorporation de « boîtes noires » sur les données produites par les maisons, avec la bénédiction des gouvernements sous le couvert de la guerre contre le terrorisme, ce prétexte-orchestre qui permet de tout justifier[155]. Edgar J. Hoover, l'ancien directeur du FBI soutenait que l'information c'est le pouvoir, ce que personne n'aurait désormais l'outrecuidance de contester. Dans le contexte actuel, il est onirique de considérer que les gouvernements vont s'abstenir d'accéder et de traiter les données personnelles médicales issues des objets connectés. Bien au contraire, dès lors que cet accès et cette collecte sont aussi aisés, il serait quasi-hérétique d'y renoncer.

La solution pourrait résider dans le cryptage des données, sans possibilités pour les gouvernements et les entreprises productrices d'objets connectés d'y

---

152 Idriss J. Aberkane, L'espionnage programmé des maisons connectées, publié sur le site lepoint.fr le 13 février 2016 : <http://www.lepoint.fr/invites-du-point/idriss-j-aberkane/aberkane-l-espionnage-programme-des-maisons-connectees-13-02-2016-2017668_2308.php>.

153 <http://www.lemonde.fr/disparitions/article/2013/07/29/mort-du-hacker-barnaby-jack-detrousseur-de-distributeur_3454728_3382.html>.

154 Idem.

155 Idem.

accéder elles-mêmes. À cet égard, une étude récente de l'Université de Harvard (rendue publique le 11 février 2016[156]) démontre que les efforts déployés par le FBI et certains législateurs visant à prohiber la vente de produits comportant une encryption ne seront pas couronnés de succès[157]. Cela est dû en partie à la profusion d'outils de cryptage disponibles hors des États-Unis, ainsi qu'au fait que des mesures telles que celles envisagées par le FBI n'empêcheraient pas les cybercriminels de trouver des logiciels d'encryption, mais, par contre, généreraient un désavantage concurrentiel pour les entreprises américaines. En toutes hypothèses, ce débat est loin d'être clos et la pondération entre la sécurité des citoyens au sens large du terme et la protection de leurs données demeure un exercice difficile. Le Privacy Shield et ses succédanés crptopolitiques vont retenir l'attention des régulateurs durant une très longue période.

3.4 L'exception culturelle française en matière d'hébergement des données de santé

L'article L1111-8 du Code de la santé publique français[158] imposait déjà à tout établissement ou professionnel de santé qui souhaitait faire héberger par un tiers des « *données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins* » de recourir à un hébergeur de données de santé à caractère personnel agréé par le Ministre de la Santé.

Le projet de loi de modernisation du système de santé français, qui vient d'être adopté le 26 janvier 2016, étend le périmètre de cette obligation à toute

156 Bruce Schneier / Kathleen Seidel / Saranya Vijayakumar, A Worldwide Survey of Encryption Products, Harvard University, Berkman Center for Internet and Society, February 11, 2016, Publication n° 2016-2, disponible à cette adresse : <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2731160##>.

157 <http://appleinsider.com/articles/16/02/12/harvard-study-says-apples-tim-cook-was-right-encryption-bans-backdoors-wouldnt-work->.

158 Disponible à cette adresse : <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072665>.

« *personne physique ou morale à l'origine de la production ou du recueil desdites données* »[159].

La réglementation française relative à l'hébergement agréé semble constituer une exception culturelle en Europe, induisant que le respect de celle-ci permettrait d'être, de facto, en conformité avec les autres réglementations européennes, réputées moins contraignantes, dont la réglementation suisse. L'ASIP Santé[160], l'organisme français en charge d'instruire les demandes d'agrément des hébergeurs de données de santé à caractère personnel, nous a confirmé qu'à sa connaissance, aucune réglementation européenne similaire à la réglementation française n'avait été adoptée.

La teneur de l'article L1111-8 du Code de la santé publique français est désormais la suivante[161] :

« *Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même, doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime.*

Les traitements de données de santé à caractère personnel que nécessite l'hébergement prévu au premier alinéa, quel qu'en soit le support, papier ou informatique, doivent être réalisés dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La prestation d'hébergement, quel qu'en soit le support, fait l'objet d'un contrat.

159 cf. art. 96-I-5° a) du projet de loi - texte n°650.

160 Soit l'Agence des systèmes d'informations partagés de santé qui est l'organe qui : <http://esante.gouv.fr/asip-sante>.

161 Depuis l'adoption de la Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

Les conditions d'agrément des hébergeurs des données, quel qu'en soit le support, sont fixées par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés et des conseils de l'ordre des professions de santé. Ce décret mentionne les informations qui doivent être fournies à l'appui de la demande d'agrément, notamment les modèles de contrats prévus au deuxième alinéa et les dispositions prises pour garantir la sécurité des données traitées en application de l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée, en particulier les mécanismes de contrôle et de sécurité dans le domaine informatique ainsi que les procédures de contrôle interne. Les dispositions de l'article L. 4113-6 s'appliquent aux contrats prévus à l'alinéa précédent.

L'agrément peut être retiré, dans les conditions prévues par l'article 24 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, en cas de violation des prescriptions législatives ou réglementaires relatives à cette activité ou des prescriptions fixées par l'agrément.

Seuls peuvent accéder aux données ayant fait l'objet d'un hébergement les personnes que celles-ci concernent et les professionnels de santé ou établissements de santé qui les prennent en charge et qui sont désignés par les personnes physiques ou morales à l'origine de la production de soins ou de leur recueil et qui sont désignées par les personnes concernées. L'accès aux données ayant fait l'objet d'un hébergement s'effectue selon les modalités fixées dans le contrat, dans le respect des articles L. 1110-4 et L. 1111-7.

Les hébergeurs tiennent les données de santé à caractère personnel qui ont été déposées auprès d'eux à la disposition de ceux qui les leur ont confiées. Ils ne peuvent les utiliser à d'autres fins. Ils ne peuvent les transmettre à d'autres personnes que celles qui les leur ont confiées.

Lorsqu'il est mis fin à l'hébergement, l'hébergeur restitue les données aux personnes qui les lui ont confiées, sans en garder de copie.

Les hébergeurs de données de santé à caractère personnel et les personnes placées sous leur autorité qui ont accès aux données déposées sont astreints au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du Code pénal.

Les hébergeurs de données de santé à caractère personnel ou qui proposent cette prestation d'hébergement sont soumis, dans les conditions prévues aux articles L. 1421-2 et L.

1421-3, au contrôle de l'Inspection générale des affaires sociales et des agents mentionnés aux articles L. 1421-1 et L. 1435-7. Les agents chargés du contrôle peuvent être assistés par des experts désignés par le ministre chargé de la santé.

Tout acte de cession à titre onéreux de données de santé identifiantes, directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions prévues à l'article 226-21 du code pénal ».

Cette disposition légale extrêmement complète constitue le résultat d'une réflexion qui n'a manifestement pas encore été diligentée dans notre pays. Elle pourrait inspirer ceux qui sont en charge de la rédaction de l'Ordonnance d'application de la loi sur le dossier électronique du patient, ce qui permettrait notamment de s'assurer :

- du sérieux et de la qualité des prestataires de services choisis ;
- d'une capacité d'intervention rapide en cas de problème dûment constaté ;
- du respect du secret professionnel et médical ;
- de la restitution des données au terme de l'hébergement ;
- de l'absence de cession à titre onéreux de données de santé identifiantes directement ou indirectement et ce même du consentement de la personne concernée.

Si l'on considère (comme le soussigné) que les données médicales sont à tout le moins aussi sensibles[162] que celles en matière bancaire ou d'assurance, il n'y aura aucune difficulté à implémenter un système similaire à celui d'agrément par la FINMA[163] prévalant actuellement en ces domaines d'activité. A défaut, des problèmes se produiront inévitablement, puisque le respect des règles légales sans contrôles efficaces et permanents est une chimère, surtout les sanctions se limitent à une recommandation.

---

162 De mon point de vue plus encore.

163 <https://www.finma.ch/fr/finma-public/etablissements-personnes-et-produits-autorises/>.

4 LE DROIT À L'OUBLI EN MATIÈRE DE SANTÉ

4.1 Le dispositif inédit français

Les anciens malades ont aussi droit à l'oubli. Cette phrase peut vous paraître singulière, mais elle reflète une réalité unique qui ne manque pas d'intérêt, dans le cadre de l'examen des normes devant régir le Big Data en matière de santé. En France, « *avant d'accorder un crédit, le banquier analysait la solvabilité de son client et, dans la majorité des cas, lui demandait de souscrire une assurance pour garantir son prêt*[164]*. L'emprunteur devait fournir de nombreuses informations, et indiquer notamment s'il avait déjà été atteint d'une affection de longue durée. En cas de réponse positive, la compagnie exigeait, afin d'évaluer les risques, tout l'historique de la maladie. Sur la base de ces informations, elle décidait ou non de proposer une couverture et fixait une éventuelle majoration de tarif*[165]*. Ce processus a exclu pendant des années de nombreux anciens malades de l'accès à la propriété* ». Le droit à l'oubli qui a fait l'objet d'un amendement au projet de loi de santé doit permettre aux anciens malades qui contractent un prêt immobilier ou un crédit à la consommation de ne plus mentionner dans leurs antécédents médicaux le cancer dont ils ont souffert[166]. Très concrètement, cela signifie qu'à la fin de l'année 2015 au plus tard, les questionnaires de santé qui accompagnent la souscription d'un crédit immobilier vont être modifiés. Ils seront rédigés de façon très précise pour respecter le droit à l'oubli. Passé un certain délai, les emprunteurs concernés n'auront plus à mentionner leurs cancers ni à répondre à des questions sur ce sujet.

---

164 Anne de Guigné, Cancer : les assureurs prêts au droit à l'oubli, article publié le 16 mars 2015, accessible à cette adresse : <http://www.lefigaro.fr/assurance/2015/03/16/05005-20150316ARTFIG00434-cancer-les-assureurs-prets-au-droit-a-l-oubli.php>.

165 Cette majoration de tarif pouvait aller jusqu'à 50%, ce qui entravait l'accès à la propriété.

166 Selon les estimations, 3 millions de personnes seraient concernées.

Ainsi, pour les contrats d'assurance de prêt, il sera instauré[167] :

- un droit à l'oubli pour les cancers survenus avant l'âge de 15 ans, 5 ans après la date de fin du protocole thérapeutique ;
- un droit à l'oubli pour toutes les pathologies cancéreuses, 15 ans après la date de fin du protocole thérapeutique ;
- une grille de référence, permettant d'assurer au tarif normal des personnes ayant contracté certains cancers, dès lors que la date de fin du protocole thérapeutique a cessé depuis un certain nombre d'années inférieur à 15 ans[168].

La loi de santé intégrant cet amendement a été votée définitivement le 17 décembre 2015[169].

Il est prévu d'étendre ce dispositif à d'autres maladies que le cancer, le protocole d'accord mentionnant explicitement cette possibilité. Les assureurs disent avoir besoin de temps pour évaluer les risques présentés par d'autres pathologies avant de les mutualiser. De nouvelles études doivent donc être menées pour rassembler des données statistiquement plus fiables sur d'autres maladies graves avant l'extension évoquée[170].

---

167 Communiqué de presse de la Fédération Française des Sociétés d'Assurance du 24 mars 2015 disponible à cette adresse : <http://www.ffsa.fr/sites/jcms/p1_1502559/fr/droit-a-loubli-une-avancee-considerable-pour-les-anciens-malades-du-cancer?cc=fn_7352>.

168 Ce sont les cancers les plus fréquents (du sein, de la prostate, etc.), pour lesquels on dispose de plus d'informations sur les taux de survie qui sont concernés.

169 Il est également intéressant de mentionner dans le contexte de cet article que la loi prévoit de regrouper dans un système national des données de santé (SNDS) les grandes bases de données médico-administratives (remboursements des soins, séjours hospitaliers, données des établissements pour personnes handicapées, causes de décès) et d'en faciliter l'accès, pour des finalités d'intérêt général, aux acteurs issus du monde associatif, des industries de santé, des assurances complémentaires et de la recherche.

170 Véronique Chocron / Edouard Lederer, Droit à l'oubli : six questions autour d'un dispositif inédit, article publié sur le site lesechos.fr le 25 mars 2015 et disponible à cette adresse : <http://www.lesechos.fr/25/03/2015/lesechos.fr/0204252469479_droit-a-l-oubli---six-questions-autour-d-un-dispositif-inedit.htm#>.

Ce dispositif inédit est clairement un moyen efficace de contrebalancer l'amélioration des modèles actuariels et prédictifs de maladies létales, comme le cancer. En ce sens, il présente un intérêt manifeste, car la démarche engagée en France permet aux assureurs d'affiner leurs processus d'évaluation du risque et aux assurés de ne pas être pénalisés *ad vitam æternam* pour des affections dont ils ont souffert. C'est en quelque sorte un processus gagnant-gagnant où les intérêts des patients-assurés sont mieux appréhendés que si les assureurs se limitaient à améliorer leurs calculs actuariels au moyen du Big Data.

4.2 Quid en droit suisse?

Le droit suisse ne connaît pas un dispositif similaire à celui qui vient d'être présenté et qui est, en réalité, unique au monde. Nous serions certainement bien inspirés d'envisager un tel dispositif nonobstant le fait que dans notre pays la souscription d'une assurance ne soit pas une obligation lors de la conclusion d'un crédit hypothécaire.

L'historique du patient a été évoqué dans le cadre de l'exemple français. Or, il existe de nombreuses possibilités d'exploitation de vos données ainsi que le décrit le Professeur Joël Colloc[171] : « *Lorsqu'il s'agit de votre santé, les requêtes dans les sites médicaux, les achats, les messages sur les réseaux sociaux permettent d'établir un profil de votre santé et de celle de vos proches.*

La déréglementation des prescriptions favorise l'automédication et transforme le patient en client ciblé par l'industrie pharmaceutique à l'aide de campagnes publicitaires. Le mésusage de certains médicaments comme le paracétamol, l'aspirine, l'ibuprofène, une méconnaissance des interactions médicamenteuses en cas d'association, des posologies à ne pas dépasser, des contre-indications et des effets secondaires font courir des risques importants d'accidents thérapeu-

171 Joël Colloc, « Santé et Big Data : l'État et les individus, impuissants face aux pouvoirs des réseaux », *L'Espace Politique* [En ligne], 26 | 2015-2, mis en ligne le 26 juillet 2015, consulté le 10 février 2016. URL : <http://espacepolitique.revues.org/3493>. ; DOI : 10.4000/espacepolitique.3493, N 52 et 53.

tiques souvent graves. La perspective de profits économiques considérables présente un intérêt bien supérieur à celui de la santé des consommateurs de ces molécules ».

Par contre, les normes actuelles applicables au patient peuvent justifier une absence de pérennisation des données. Les données qui ne sont plus nécessaires au maître du fichier doivent être détruites[172]. Ainsi au-delà du délai de conservation qui est d'ordinaire de 10 ans[173], cette démarche devrait être automatisée et sanctionnée en cas de non-respect de l'incombance[174]. Ce droit à l'oubli existe donc sous une autre forme dans la jurisprudence[175] également, via le principe de finalité qui exige que les données personnelles ne soient traitées que dans le but indiqué lors de leur collecte, qui est prévu par loi ou ressort des circonstances[176], ainsi que via le principe de proportionnalité (art. 4 al. 2 LPD). Il paraît également important de rappeler, même si les procédures sont rarissimes, qu'il est possible sur la base de l'article 15 al. 1 LPD de conclure à la destruction des données personnelles devenues notamment inutiles.

Auparavant, soit durant les 10 ans, il est loisible aux professionnels de santé de ne conserver qu'une version électronique avec un bémol : les médecins sont encouragés à conserver pendant au moins dix ans les originaux des dossiers médicaux (s'ils existent sous forme papier), des formulaires de consen-

172 Le PFPDT s'exprime en ces termes s'agissant de la conservation des données médicales dans son Guide relatif aux traitement des données personnelles dans le domaine médical, Traitement des données personnelles par des personnes privées et des organes fédéraux, p. 25 : « *La LPD n'indique pas combien de temps il faut conserver les données relatives à la santé dans le domaine privé. Pour cette raison, le principe de la proportionnalité est ici applicable. Selon ce principe, les données dont on n'a plus besoin doivent être détruites. Les dispositions fédérales et cantonales particulières en matière de conservation des dossiers dans le domaine médical ou à des fins statistiques sont réservées* ».

173 Notamment dans les Cantons de Berne, Zurich et du Valais.

174 Sur le plan disciplinaire à tout le moins, une action civile du patient demeurant réservée.

175 ATF 122 III 449, JT 1998 I 131, ATF 109 II 353, JT 1985 I 98.

176 Art. 4 al. 3 LPD.

tement éclairé ou de levée du secret médical pour des motifs liés à la preuve en cas de litige avec le patient[177].

Selon l'expression consacrée, le médecin doit donc détruire ou rendre au patient les dossiers médicaux à l'échéance du délai de conservation. Il peut même en certaines circonstances devoir détruire les données avant l'échéance de ce délai à la demande du patient[178]. S'il est relativement aisé de s'assurer qu'aucun dossier physique n'est conservé, il en va différemment en présence d'un dossier électronique.

Quid en cas de dossier électronique du patient, respectivement de dossier médical informatisé[179] détenu par une assurance, un Canton ou une société privée? Comment s'assurer que des données ne seront pas conservées, ne serait-ce qu'à des fins statistiques ou d'étude ?

Le PFPDT recommande relativement aux dossiers papier une destruction dans son propre déchiqueteur à papier soit d'en constater soi-même la destruction au sein d'une centrale d'incinération des ordures[180]. Cela signifie donc qu'en cas de destruction d'un dossier électronique, le professionnel de santé doit lui-même s'assurer de l'effacement définitif. Il ne suffit donc pas d'intégrer le dossier à la corbeille de l'ordinateur. Bien au contraire, le maître de fichier doit pouvoir démontrer la destruction définitive et seule l'utilisation d'un logiciel spécialisé est à même de remplir ces conditions. La preuve de la destruction lui incombe au demeurant.

---

177 Conservation des dossiers médicaux, originaux ou sous forme électronique, Association des Médecins du Canton de Genève, disponible à cette adresse : <http://www.amge.ch/2014/10/09/conservation-du-dossier-medical-documents-originaux-ou-sous-forme-electronique/>; le conseil relatif à la conservation des originaux pendant 10 ans a été donné par le Professeur Philippe Ducor, Avocat-conseil de l'AMG.

178 Jugement tessinois, Rivasta ticinese di diritto, II-2012, p. 51, n° 10, CPD 7.6.2010.

179 Relativement à cette notion, Sabrina Burat, La télémédecine et le droit suisse, Analys au regard du droit contractuel, de la Loi fédérale sur la protection des données, de la responsabilité civile et des assurances sociales, Neuchâtel 2012, p. 197 et 198.

180 Guide relatif au traitement des données personnelles dans le domaine médical, Traitement des données personnelles par des personnes privées et des organes fédéraux, p. 25.

Il y a une impérieuse nécessité de déterminer dans la loi[181] les conditions d'exercice d'un droit à l'oubli s'agissant des données médicales. Le développement du Big Data va générer une multiplication des bases de données relatives à la santé et sans réglementation rapide, simple et uniforme, obtenir un droit à l'oubli des données médicales deviendra une gageure.

5 CONCLUSIONS ET PERSPECTIVES

Comme le relève le Professeur Bertil Cottier, il est important de pouvoir renforcer les capacités d'action du PFPDT, spécifiquement lorsque des données sensibles sont traitées en si grand nombre : « *Le Préposé doit pouvoir sanctionner et régler rapidement de nouveaux défis* »[182]. De surcroît, dans la configuration actuelle et à l'aune du budget infinitésimal (compte tenu des tâches à accomplir et de leur complexité), de ses pouvoirs d'investigations limités[183] et de l'absence de réelle sanction, le PFPDT peut être considéré comme David au regard des moyens dont disposent les Goliaths qui lui font face.

La quasi-loi d'opérette qu'est la LPD[184] doit faire place à des dispositions qui, à l'instar de ce qui se passe chez nos voisins français et espagnols, permettent de sanctionner sévèrement les abus et de devenir un outil préventif efficace. À défaut, notre pays attirera tous les acteurs désireux de se soumettre à une régulation light, avec pour conséquence à terme, le risque que nos voisins considèrent que la Suisse ne dispose plus d'un niveau adéquat de protection des données. À cet égard, les députés français viennent d'adopter des dispositions renforçant considérablement le pouvoir de coercition de son gardien

181 La loi sur le dossier électronique du patient, mais également les normes cantonales relatives à la santé.

182 Interview de Bertil Cottier sur le projet de révision de la LPD, in : plaidoyer 1/16, p. 14.

183 Le PFPDT peut se faire présenter un traitement de données, mais pas diligenter des vérifications inopinées, alors que la CNIL son pendant français a ce pouvoir et l'a utilisé à bon escient notamment pour procéder à des vérifications relativement aux Google Cars.

184 Avec la seule possibilité d'émettre des recommandations.

des données, la Commission Nationale de l'Informatique et des Libertés (CNIL[185]) :

Le texte prévoit des sanctions pécuniaires[186] :

- De 10 millions d'euros maximums ou, pour les entreprises, jusqu'à 2% de leur chiffre d'affaires annuel mondial « *réalisé lors de l'exercice précédant l'exercice au cours duquel le manquement a été commis* » – pour tous les manquements au chapitre IV et aux articles 34 à 35 de la loi Informatique et Libertés (non-respect des formalités préalables à la mise en œuvre des traitements, violation des obligations concernant la sécurité des données stockées par le responsable d'un traitement, etc.).
- De 20 millions d'euros maximum ou, pour les entreprises, jusqu'à 4% de leur chiffre d'affaires annuel mondial – pour tous les autres manquements.

Concrètement et si ce texte est maintenu au Sénat, cela signifie que les géants du Net s'exposeront à des sanctions bien supérieures à 20 millions d'euros. Google Inc., avec ses 66 milliards de dollars de chiffre d'affaires pour l'année 2014, pourrait, théoriquement, se voir infliger une amende de plus de 2 milliards d'euros à l'aune de ces dispositions ! Voilà qui semble un tantinet plus dissuasif qu'une recommandation du PFPDT… À cet égard, la question formulée par le Conseiller national Fahti Derder le 2 décembre 2015 mérite notre attention : « *Le mandat du préposé fédéral à la protection des données doit-il être adapté à la révolution du ‹ Big Data› ?* »[187]. La Présidente de la Confédéra-

185 <http://www.cnil.fr>.

186 Xavier Berne, Loi Numérique : la CNIL pourra infliger des amendes de 20 millions d'euros, article du 22 janvier 2016 publié sur le site NextImpact : <http://www.nextinpact.com/news/98192-loi-numerique-cnil-pourra-infliger-amendes-20-millions-d-euros.htm>.

187 Voici le libellé exact du texte déposé : « La quantité de données émises par les citoyens est en très forte croissance. Nous émettons de plus en plus de données, de plus en plus sensibles et le plus souvent inconsciemment (‹ Big Data ›). La défense des libertés fondamentales de l'individu - plus menacées que jamais - devient une priorité de notre État de droit, et le poste de pré-

tion Simonett Sommaruga a répondu à cette question pertinente en ces termes[188] : « *Conformément au mandat du Conseil fédéral du 1er avril 2015, le Département fédéral de justice et police est chargé d'élaborer un avant-projet de révision de la loi sur la protection des données d'ici à fin août 2016. L'avant-projet tiendra compte, notamment, des réformes en cours au sein de l'Union européenne et du Conseil de l'Europe. Il est prévu que la question des tâches et des moyens du préposé fédéral à la protection des données et à la transparence soit examinée dans ce cadre. Je vous informe également que la question des tâches et des moyens du préposé est abordée dans l'esquisse d'acte normatif relatif à la révision de la loi sur la protection des données. Le rapport est disponible sur le site Internet de l'Office fédéral de la justice, si cela vous intéresse* ». En réalité si la réponse est correcte, elle ne prend pas en considération le fait que l'analyse juridique relative au Big Data n'interviendra qu'ultérieurement dans le cadre des travaux de la Commission Rechsteiner et qu'il sera donc impossible lors de la rédaction de l'avant-projet attendu pour août 2016 d'intégrer à la réflexion à conduire sur les moyens du PFPDT une quelconque quote-part liée à l'activité topique à déployer en relation avec le Big Data.

En matière de Big Data, hormis les sanctions précitées, il est important et urgent qu'une analyse juridique intervienne dans le cadre de la révision de la LPD, respectivement de la rédaction de l'avant-projet de loi par l'OFJ et dans le cadre des travaux de la Commission Rechsteiner. L'argument développé par le groupe d'accompagnement ne résiste pas à un examen sérieux. La doctrine a analysé en détail les risques inhérents au Big Data, certes pour certaines publications ultérieurement à la remise du rapport du 29 octobre 2014. Le sujet a atteint un degré de maturité suffisant. À cela s'ajoutent les résultats de l'étude commandée par l'OFCOM qui démontrent, rien de moins qu'un dysfonctionnement du marché actuel des données. Lorsqu'un marché dont le fonctionnement est susceptible de porter atteinte aux droits de nombreuses personnes dysfonctionne, d'ordinaire, on le régule immédiatement !

---

posé fédéral à la protection des données prend une ampleur inédite. Ne faut-il pas, dans ce contexte, revoir le mandat du préposé et lui donner plus de moyens? ».

188 <http://www.parlament.ch/ab/frameset/f/n/5001/483658/f_n_5001_483658_483726.htm>.

L'évolution du régime juridique du Big Data dépendra principalement de la capacité de mobilisation des acteurs d'ici à la fin 2017. Si aucun *habeas corpus* n'est proposé, les normes métiers auront pris l'ascendant et imposer ensuite des standards juridiques provoquera une levée de boucliers de l'économie qui est compréhensible. La stagflation du dossier électronique du patient doit inciter les autorités et les politiques à envisager une réglementation plus prolixe, pour éviter une perte de confiance ultérieure nocive au développement d'un secteur d'activités si important pour la Suisse. À défaut, d'autres pourraient nous imposer ce que nous n'avons pas su bâtir préventivement, ainsi que cela a été le cas dans le domaine bancaire.

En matière de données médicales spécifiquement, l'attention doit être portée sur une uniformisation des pratiques dans le respect du principe du fédéralisme portant à tout le moins sur des standards de sécurité minimaux. À l'échelle d'un pays comme la Suisse peut-on encore s'offrir le luxe d'avoir des systèmes d'information qui diffèrent d'un Canton à l'autre ? Quand la sécurité des patients est en jeu, la prise de risque du recours à des prestataires étrangers paraît de ce point de vue une entreprise téméraire pour reprendre un concept bien connu des assureurs. La France a réglé ce problème de manière quasi-définitive dans le cadre de l'obligation d'être agréé par le Ministère de la Santé, lorsque l'on veut héberger de telles données. À ce jour, cette solution paraît la plus pertinente pour éviter les vols et les pertes de données. Puisse cette option être rapidement envisagée dans notre pays, notamment en ce qui concerne le dossier électronique du patient !