Vers un droit collectif sur les données de santé

Danièle Bourcier, Primavera de Filippi

Vers un droit collectif sur les données de santé

Danièle Bourcier
Directrice de recherche émérite

Primavera de Filippi
Chargée de recherche

CERSA / CNRS / Université Paris II

Introduction

La révolution du Big data multiplie les pratiques de recueil de données dans tous les secteurs professionnels et provoque une nouvelle explosion de la masse de données disponibles. Mais c'est certainement dans le domaine de la santé, où les applications se sont développées le plus massivement[1], que les données à la croisée du secteur public et du secteur privé suscitent le plus de questions sur leur statut et sur leur partage au moment de la mise en application de l'Open data[2]. En effet ces données relèvent à la fois du bien commun de l'humanité et du plus profond de l'intime. Ce sont des données à caractère personnel et catégorisées comme sensibles, voire ultra sensibles. Autre date importante : celle de l'entrée en vigueur du Règlement général européen sur la protection des données (RGPD)[3] qui oblige à s'interroger sur le régime de protection de cette catégorie particulière de données, définies justement pour la première fois dans un texte normatif, les "données de santé".

---

[1] En France, l'ensemble des données recueillies par le secteur public sont regroupées au sein du Système national des données de santé (SNDS). Les bases de données de l'assurance maladie (SNIIRAM) cohabitent avec celles des hôpitaux (PMSI). Y transitent chaque année quelques 1,2 milliards de feuilles de soins, 500 millions d'actes médicaux et 11 millions de séjours hospitaliers. Ce système sera enrichi de données concernant les causes médicales de décès en juin 2017, des données relatives au handicap à partir de 2018, et enfin, d'un échantillon de données fournis par les organismes complémentaires en 2019.

[2] Le 7 avril 2018, le 1° de l'article de la loi Numérique qui introduit ce principe d'Open Data « par défaut » dans notre droit (à l'article L312-1-1 du Code des relations entre le public et l'administration pour être précis), est entré en vigueur. À partir du 7 octobre 2018, les administrations devront également mettre en ligne les « principaux documents » qu'elles doivent répertorier au titre de l'article L322-6 du CRPA et diffuser toutes leurs "bases de données », ainsi que les données « dont la publication présente un intérêt économique, social, sanitaire ou environnemental » (ainsi que leurs mises à jour).

[3] Le cadre législatif en France est défini par la loi Informatique et Libertés du 6 janvier 1978 modifiée en 2004 par la transposition de la directive européenne 95/46/CE du 25 octobre 1995. Cette directive a été remplacée par le Règlement européen sur la protection des données (Dit RGPD) UE 2016/679 du 27 avril 2016 qui est entré en vigueur le 25 mai 2018 dans l'ordre normatif des 28 Etats membres. La mise à jour (il n'y a pas de transposition) de la loi de 1978 sera effectuée avant le 1er janvier 2019.

Ce régime de protection est fondé sur le principe d'une interdiction générale de la collecte des données de santé. Cette interdiction peut être levée par le consentement éclairé et exprès du patient ou dans le cadre de la sécurité sociale, la médecine préventive et pour des intérêts de santé publique. L'application de ce règlement constitue un pas décisif vers une meilleure défense de notre vie privée et les réactions qu'il suscite de par le monde[4] en sont un témoignage. Mais l'efficacité de ce régime est déjà contestée en ce qu'elle n'assurerait pas une protection technique et juridique suffisante. En effet, compte tenu des pratiques en ligne et de l'évolution des techniques, d'abord nous sommes de plus en plus incités à donner notre consentement pour accéder aux plateformes sans que celui-ci soit explicite, informé et exprès, et sur le deuxième point, l'anonymat ne semble plus garanti de façon absolue en l'état actuel des techniques de cryptographie, compte tenu des possibilités de réversibilité en informatique. Dans un ouvrage précédent[5], nous avions évoqué la possibilité de créer un "service public de la donnée". Mais cette idée n'a pas, jusqu'à présent, été reprise.

Alors comment peut-on élargir la réflexion sur la protection des données de santé? Il existe plusieurs façons de protéger les données: un droit personnel fondé sur les libertés fondamentales et l'exclusivité issue du régime de la propriété. Ces deux options résolvent certains problèmes mais en suscitent d'autres.

Nous nous proposons donc d'explorer une autre solution qui pourrait dépasser les inconvénients de ces options. Nous voudrions d'abord les distinguer pour mieux comprendre leur limites réciproques, liées à une vision individualiste des données de santé. Puis nous suggérons en conclusion de reconnaître un droit collectif sur ces données plutôt qu'un droit individuel. Nous excluons ainsi leur patrimonialisation (droit de propriété sur les données) option souvent proposée actuellement comme alternative, mais en retour cette solution n'assure pas une bonne protection collective. Ce droit collectif doit donc être protégé non pas par une droit de propriété (fondée sur l'exclusivité) ou par un droit personnel (fondée sur le consentement) mais comme une ressource commune dont la protection doit être garantie par l'Etat.

I- Données personnelles et données de santé: une définition précisée mais extensive

A l'heure des Big data, les données doivent être spécifiées par domaine d'application (fiscalité, *smart city,* …). La santé est un secteur d'activité qui nécessite par excellence des conditions et contraintes particulières. De plus ces données se trouvent à l'intersection des données

[4] Ce texte européen est applicable aux entreprises établies sur le territoire européen ou qui recourent à des moyens de traitement situés sur le territoire européen

[5] D. Bourcier & P. De Filippi (sous la direction de) *Open Data Big Data Nouveaux défis pour la vie privée,* Mare et Martin, 2016.

scientifiques[6] et des données pratiques qu'elles soient issues de la pratique hospitalière ou de la médecine de ville. Elles concernent le secteur public mais aussi le secteur privé et elles sont hautement *monétisables.*

Accroissement des sources de données de santé

Les données de santé renvoyaient traditionnellement à une information sur l'état de santé de la personne lors d'un parcours de soin. Aujourd'hui le domaine de la santé devient une application privilégiée du Big data notamment avec l'internet des objets. De plus avec l'apprentissage machine (*deep learning*), la recherche médicale est devenue l'objet d'une algorithmisation généralisée facilitant les comparaisons entre des milliers de dossiers et des raisonnements inductifs ou prédictifs vers de nouveaux traitements. Ainsi en 2016, une patiente atteinte d'une leucémie rare a pu être sauvée grâce au logiciel Watson (IBM) qui en un temps très court a identifié, parmi des millions de données en ligne, la maladie et trouvé le nouveau traitement qui l'a sauvée.[7]

La notion de données de santé est désormais définie de manière large par le RGPD et elle devient commune aux Etats de l'Union européenne : " *Les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique y compris la prestation de services de soins de santé qui révèlent des informations sur l'état de santé de cette personne".*

En France cette notion recouvre non seulement l'ensemble des données découlant des parcours de soins mais aussi celles qui, détenues par d'autres acteurs qu'ils soient techniciens (par exemple les développeurs informaticiens) ou administratifs (par exemple les gestionnaires de droits sociaux) constituent une information sur l'état de santé de la personne. Ainsi le régime des données de santé ne relèvent pas seulement de la Loi Informatique et Libertés. Elles concernent les Dispositions sur le secret (art. L. 1110-4 du CSP) ; celles relatives aux référentiels de sécurité et d'interopérabilité des données de santé (art. L. 1110-4-1 du CSP) ; à l'hébergement des données de santé (art. L. 1111-8 et R. 1111-8 et s. du CSP) et à leur mise à disposition (art. L1460-1 et s. du CSP) ; enfin elles doivent aussi être soumises à certaines interdictions comme celle de l'Interdiction de procéder à une cession ou à une exploitation commerciale des données de santé (art. L. 1111-8 du CSP, art. L 4113-7 du CSP).

Développement de la médecine personnalisée à partir de données personnelles hétérogènes

En octobre 2013, l'autorité de régulation américaine des médicaments et des dispositifs médicaux (la *Federal Food and Drug Administration*, FDA) a précisé ce que recouvrait la médecine personnalisée et sur quelles données elle se fondait : a) les résultats de l'imagerie

---

[6] voir Elias Zerhouni, « Les grandes tendances de l'innovation biomédicale au XXIe siècle », Paris, Collège de France, coll. « Leçons inaugurales », n° 217, 2011, http://lecons-cdf.revues.org/434, [DOI] 10.4000/lecons-cdf.434l Pour lui la médecine de demain sera *prédictive*, *personnalisée*, *préemptive* et *participative*.

[7] Cité dans A.Basdevant & J.-P. Mignard, *L'empire des données ,Essai sur la société, les algorithmes et la loi,* Don Quichotte, 2018 p.80.

médicale, qui permettent d'adapter les traitements à partir de données anatomiques et physiologiques des patients b) la diffusion massive des téléphones portables qui favorise le développement de données captées pour l'e-santé en général c) les données issues de biocapteurs individuels, ce que l'on appelle le *Quantified Self* ou la "mesure du soi" : chaque individu enregistre lui-même en continu certains de ses paramètres afin de suivre son état de santé d) les données générées par les plateformes en ligne, qui recueille et partage des informations de santé, du type Genomera, PatientsLikeMe, Cancer Commons, et developpent des pratiques de *self-monitoring* e) le développement de la médecine régénératrice et des recherches sur les cellules souches. Les thérapies personnalisées relèvent principalement de la génétique mais la définition génomique de la médecine personnalisée inclut des approches plus extensives.

Des nouvelles données à caractère personnel : les données génétiques

Le Règlement a inclus de nouvelles données de santé particulièrement sensibles : les données génétiques dont voici la définition : "*Données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résulten*t, notamment, d'une *analyse d'un échantillon biologique de la personne physique en question*".[8]

Besoin d'élargissement de la notion de "donnée personnelle"

En revanche, la notion de "personne concernée" (article 38 de la loi de 1978) n'a pas été étendue à d'autres personnes que celles dont les données font l'objet d'un traitement direct.[9] Pourtant de plus en plus dans un monde en réseau, on s'aperçoit que les données sont de moins en moins "personnelles". En effet beaucoup d'informations personnelles ne sont pas liées à un individu mais à une lignée généalogique. C'est donc tous les membres de sa famille voire de son ethnie qui devraient donner le consentement demandé. Certains ont même proposé la notion de "données collectives pluripersonnelles" qui viserait l'écosystème dans lequel est inséré la personne[10]. Plus largement, la notion de "données personnelles" sur laquelle est fondée tout le régime de protection devient inadaptée à l'heure des données connectées (*linked data)*. Elle est devenue contestable dans la mesure où chaque noeud du réseau est relié tous les liens et noeuds du réseau donc avec les données personnelles d'autres personnes. Ces données sont devenues relationnelles. La subjectivation de ce droit devient obsolète par rapport aux caractéristiques relationnelles des données et par rapport à la personnalisation d'un droit de recours.

---

[8] Article 4 du RGPD

[9] D.Bourcier, "Réflexion éthique sur le partage des données en science: entre communs scientifique et Open data" in *Open data & Big data Nouveaux défis pour la vie privée* (D. Bourcier & P. De Filippi eds), Mare& Martin, 2016 p.234.

[10] I. Coulybaly, *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, Thèse Université de Grenoble, 2011.

II - De la loi française au Règlement européen: un régime plus protecteur des données de santé

La Loi française: les bases du régime

La loi de 1978 caractérisait les données de santé comme des données sensibles qu'il était interdit de collecter ou de traiter (Article 8) mais elle n'en donnait pas de définition. Le traitement est en principe interdit sauf lorsque le consentement de la personne a été obtenu ou que la finalité du traitement est conforme aux exceptions prévues par la loi.

Ainsi dès lors que la personne concernée par le traitement de données de santé donne son consentement exprès, le traitement est autorisé. Pour qu'il soit considéré comme valable, la loi veille à ce que l'utilisateur soit informé de la finalité du traitement c'est à dire du cadre où les données seront utilisées. Le traitement des données personnelles de santé est en revanche autorisé et ce, sans consentement préalable de l'utilisateur s'il poursuit notamment une des finalités suivantes :

- gestion des systèmes et services de santé ou de la protection sociale
- préservation de la santé publique (pour éviter notamment la propagation des maladies)-
- appréciation médicale : soins, diagnostics, médecine préventive,
- préservation des intérêts vitaux d'une personne en incapacité de donner son consentement

L'utilisation de ces données est donc relativement restreinte et, *de facto*, ces dernières ne peuvent faire l'objet d'une commercialisation. Une autre interdiction concernant les données personnelles des médecins prescripteurs a d'ailleurs été insérée dans la loi.[11] La loi française avait déjà fixé les règles de base concernant les données relevant du secteur de la santé.

Il faut cependant que cette loi soit réorganisée en fonction des apports du RGPD. Avant l'entrée en vigueur du RGPD, le projet de loi gouvernemental de mise à jour[12] a soulevé de la part de la CNIL et du Conseil d'état quelques observations qui rencontrent les réflexions que nous avons soulevées dans cet article. Ces deux institutions ont remarqué qu'une simple transposition sans modifier l'architecture de la loi rendrait le texte illisible et à cette occasion, a été proposée la création d'un Code du numérique et des libertés. Enfin ces institutions se sont étonnées de

[11] Sans préjudice des dispositions de la loi n° 78-17 du 6 janvier 1978, le code de la sécurité sociale a émis une autre interdiction protégeant les données personnelles du personnel médical prescripteur. "Sont interdites la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des informations médicales mentionnées à l'article L. 161-29 du code de la sécurité sociale, dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur."

[12] présenté au Conseil des ministres le 13 décembre 2017.

l'absence de considérations éthiques sur des questions soulevées par les innovations techniques dans le domaine de la médecine comme:

- Le traitement massif des données;
- L'absence de réflexion sur la propriété (ou l'inappropriation) des données de santé détenues ou élaborées;
- La maîtrise et le contrôle des algorithmes;
- L'assistance aux actions humaines procurées par des moyens informatiques.

Ce sont certaines de ces réflexions que nous explorons dans la suite de cet article.

Les apports et impacts du RGPD

Le Règlement a abordé les données de santé plus précisément que la loi française. Il en a proposé une définition légale bien que cette définition à l'heure du Big data semble déjà trop étroite. Mais surtout il introduit un régime de dérogation à la levée du consentement ce qui conduira certainement les Etats membres à introduire des conditions supplémentaires d'ouverture quand il s'agit de données personnelles de santé. Ainsi un opérateur pourrait se voir obligé de demander une autorisation à la CNIL - comme avant le RGPD - pour un traitement exécuté dans le cadre d'une mission d'intérêt public. Les autorités publiques hésitent visiblement entre un régime de libération et d'ouverture des données (il y en a tant) et des restrictions d'usage fondées sur la conception d'un "ordre public sanitaire"[13]. Le danger est que les pouvoirs publics ne peuvent avoir une politique plus restrictive à l'heure de l'Open data que les *Big pharmas* et les réseaux industriels de santé. C'est d'ailleurs face à cette politique hésitante que des Communs entre scientifiques se sont développés dans le domaine de la santé sous le nom de data-sharing[14]. En 1996, des chercheurs, impliqués dans le séquençage du génome humain, ont ainsi signé un ensemble d'accords, les Principes des Bermudes, consacrant les bases du partage ouvert des données pré publiées. La première définition de l'Open data a été donnée par la Déclaration internationale sur le libre accès de Budapest qui s'est tenue le 14 février 2002, connue sous

[13] S. Hennette-Vauchez, *Disposer de soi? Une analyse du discours juridique sur les droits de la personne sur son corps*, L'Harmattan, 2014.Cette thèse propose comme solution un "ordre public corporel" comme sauvegarde ultime de la dignité de la personne humaine à l'heure des technologies nouvelles dans ce domaine. Le rapport entre la personne et son corps est vu sous l'angle du monisme ou du dualisme mais à aucun moment la donnée de santé n'est impliquée dans le rapport entre corps et personne (le Big data n'est pas encore advenu).

[14] "Les enjeux éthiques du partage des données scientifiques", Avis du COMETS (7 mai 2015)

l'acronyme *BOAI (Budapest Open Access Initiative).* De là, de nombreuses autres initiatives vont voir le jour ailleurs dans le monde avec par exemple la Déclaration de Berlin de 2003 sur le libre accès à la connaissance dans toutes les sciences y compris les sciences humaines. La plupart des organismes scientifiques ont souscrit à ces déclarations et légitimé cette culture de l'accès ouvert. Enfin en 2013 une initiative issue du domaine de la biologie humaine a lancé la « Global alliance for genomics and health » destiné à gérer des millions de génomes par des dizaines de milliers de volontaires.

Enfin les règles concernant le consentement, défini plus précisément que dans la loi de 1978[15] ont été renforcées. Ainsi, avant d'obtenir le consentement de la personne concernée, celle-ci doit être parfaitement informée sur les « finalités » de la démarche : quel est l'usage de ses données, combien de temps seront-elles conservées, etc. ?

De plus l'accord obtenu doit être sans ambiguïté. Il faut qu'il soit "matérialisé" » dans un texte (pas de case cochée à l'avance), pour pouvoir, en apporter la preuve concrète. Aucun accord verbal ne peut être validé. Précisons enfin que ce consentement peut être à tous moments retiré. Cet aspect que nous discuterons plus loin montre que les données ne sont pas entièrement disponibles et compromet déjà toute tentative de les patrimonialiser.

III- Comment maîtriser le traitement des données de santé à l'ère du big data?

L'évolution tant de la notion que du régime juridique des données personnelles de santé nous conduit à discuter de l'avenir de leur statut, que le RGPD a remis à l'ordre du jour.

Droit personnel : protection de la vie privée et données personnelles

On a vu que la loi française prévoit des cas où les données personnelles appartiennent à certaines catégories dites "sensibles" et sont sujettes à un niveau de protection plus élevé. Les données de santé appartiennent à l'une de ces catégories, dans la mesure où elles reflètent les aspects les plus intimes de la personne. Les règles qui régissent la façon dont les individus peuvent disposer de

[15] "Manifestation de volonté libre, spécifique, éclairée, univoque, par laquelle la personne concernée accepte par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fasse l'objet d'un traitement".

ces données sont donc plus restrictives que celle qui constituent le régime général des données personnelles. La protection des données personnelles est fondé sur le droit à la protection de la vie privée [16]: un droit fondamental qui permet à tout individu de se prévaloir de certaines prérogatives et pouvoirs dans le but de préserver l'intimité de sa sphère privée. Il s'agit donc là d'un droit subjectif, inséparable du sujet de droit. Ce droit est opposable en justice et permet aux individus de limiter le pouvoir d'action des tiers.

Alors que le traitement des données personnelles - y compris les données de santé - est interdit par défaut, les individus ont le droit de décider par eux-mêmes de la façon de disposer de leurs droits en autorisant des acteurs à traiter certaines typologies de données, pour des finalités précises. Le consentement réside donc au cœur du droit sur la protection des données personnelles, comme élément permettant de renoncer à l'exercice de ce droit dans des situations prédéfinies.
Or, en vue du caractère personnel de ce droit, le consentement peut être révoqué, à tout moment, sans besoin d'aucune justification. Ainsi les acteurs responsables du traitement ne peuvent pas s'emparer des données personnelles et ne peuvent surtout pas revendiquer un droit de propriété sur ces données. Cela est illustré, notamment, par les limitations portant sur la conservation des données personnelles collectées suite au consentement des personnes concernées, dont la durée de conservation doit être préalablement définie par le responsable du traitement.
Ainsi, le droit sur la protection des données personnelles, tel qu'il a été consacré par la Loi Informatique et Libertés du 6 janvier 1978 "*ne repose pas sur une logique patrimoniale mais sur une logique de droits attachés à la personne*".[17] Les données personnelles ne représentent donc pas une ressource dont les individus sont propriétaires, mais uniquement une extension de leur personnalité, dont ils ont le droit de contrôler l'usage et l'exploitation.
À la différence des droits réels ou patrimoniaux (*in rem*) associés à des choses corporelles ou incorporelles, et des droit personnels (*in personam*) attachés à des individus et qui ne peuvent être exercés que à l'encontre de ces individus, le droit à la protection de la vie privé retombe dans la catégorie des droits *extra-patrimoniaux*. Comme les droits patrimoniaux, ces droits sont opposables envers tout le monde (et non seulement envers des individus spécifiques). Mais les droits extra-patrimoniaux se distinguent des droits patrimoniaux dans la mesure où ils ne sont pas associés à des choses. Ces droits sont inhérents à la personne humaine et ne peuvent donc pas en être dissociés. Ce sont des droits fondamentaux, qui visent à protéger la dignité humaine, et dont on ne peut donc pas disposer librement. C'est pour cela que les individus n'ont pas le droit de

[16] Pour G. Braibant, la catégorie de données personnelles est plus large que celle de vie privée voir Rapport, 1998 DONNEES PERSONNELLES ET SOCIETE DE L'INFORMATION Rapport au Premier Ministre sur la transposition en droit français de la directive no 95/46 le 3 mars 1998.
[17] Cf. Les rapports du Conseil d'État (ancienne collection Étude et documents du Conseil d'État) "Le numérique et les droits fondamentaux" (2014), p. 263.

renoncer à leur droit sur la protection de la vie privée : il s'agit d'un droit fondamental inaliénable.

Le principe d'indisponibilité des données à caractère personnel a été reconnu à plusieurs reprises par le Conseil d'État, qui précise que "*s'il convient de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant celui-ci comme un droit à l'autodétermination plutôt que comme un droit de propriété*".[18]

Sur ce point, il est important de rappeler que le droit de propriété se compose de trois droits distinct: (1) l'*usus*, ou le droit d'utiliser librement une ressource; (2) le *fructus*, ou le droit de récolter les fruits issus de cette ressource; (3) l'*abusus*, ou le droit de disposer de cette ressource - soit en la transférant à des tiers, soit en la détruisant. Dans le cas des données personnelles, les sujets de droits ne peuvent bénéficier que de l'usufruit (*usus* + *fructus*) de leurs données personnelles. Ils ne sont, cependant, pas propriétaires de ces données car il ne peuvent pas en disposer librement (*abusus*).

Ce principe est illustré, en partie, par les règles concernant le droit à la portabilité des données personnelles, reconnu par l'Article 20[19] du Règlement européen sur la protection des données personnelles. Ce droit permet aux individus de récupérer (ou de transférer) toutes les données les concernant, lorsque celles-ci sont détenues par des prestataires de services. Ainsi, malgré le fait que ces individus ont consenti à la collecte et au traitement de ces données, sont maintenus néanmoins le droit d'accéder à ces données et le droit d'être tenu au courant de toutes les utilisations qui en sont faites. Le but est d'éviter que, une fois le consentement donné, les personnes concernées ne puissent plus révoquer ce consentement, par crainte de perdre l'accès à leur données.

Une restriction supplémentaire existe pour les données personnelles qui retombent dans la catégorie des données de santé, pour lesquelles le principe d'indisponibilité s'accompagne de l'interdiction de procéder à une cession ou à une exploitation commerciale des données. Le code de la santé publique (CSP)[20] précise en effet que "*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*."

Il semblerait ainsi que, dans le contexte des données de santé, les individus ne bénéficieraient que d'un *usufruit partiel* de leur données personnelles, puisque la loi interdit à tout acteur de commercialiser les données de santé, indépendamment du consentement des personnes concernées. (Il est à noter que cela n'empêche pas la commercialisation des données dérivées ou des résultats issus du traitement de ces données, dans la mesure où ceux-ci ont été correctement anonymisés).

---

[18] Cf. Les rapports du Conseil d'État (2014), op.cit. p. 263.

[19] Article 20 du RGDP: "Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle"

[20] Voir art. L. 1111-8 et art. L 4113-7 du CSP.

Alors que ces limitations puissent paraître comme une restriction à la liberté des individus, il s'agit en fait d'un mécanisme qui permet de les protéger contre une exploitation abusive de leurs données. S'il était possible de disposer librement de ces droits, les personnes concernées n'auraient plus le droit de contrôler l'exploitation qui est faite de leurs données, même si ces utilisations vont à l'encontre de leur dignité.

Enfin, il existe aussi des justifications morales ou éthiques au principe d'indisponibilité des données de santé. Pour les mêmes raisons que la loi interdit de monnayer certaines parties ou produits du corps humain (tels que les organes ou le sang), les données de santé (qui sont une information sur le corps de la personne) ne devrait pas, elles aussi, être commercialisées.

La critique qui est souvent faite au cadre juridique actuel sur la protection des données personnelles est que le consentement - bien qu'il soit explicite et informé- ne reflète pas les intérêts réels des individus.[21] Cela est particulièrement vrai sur Internet, où toute interaction avec un prestataire de service ne peut se faire qu'après avoir consenti à une politique de confidentialité des données qui est souvent très large et peu protectrice de la vie privée des utilisateurs de la plateforme. Avec l'arrivée du Big data et de l'apprentissage machine, la situation s'est encore aggravée. Étant donné la centralité des donnés dans les algorithmes de recommandation ou de personnalisation, et la nécessité d'agréger un maximum de données hétérogènes comme nous l'avons vu, dans le but d'affiner les processus de catégorisation ou de profilage des individus, tout internaute désirant aujourd'hui bénéficier d'un service personnalisé n'a plus la possibilité de s'opposer à la collecte et au traitement de ses données personnelles.

Droit de propriété sur les données: avantages et inconvénients

Face à ces critiques, certains acteurs ont proposé une approche alternative à la protection des données personnelles, fondée sur une logique patrimoniale. Lawrence Lessig a été un des premiers partisans de cette approche, en développant dans son article "Privacy as Property" (2002) l'idée de conférer un véritable droit de propriété sur les donnés personnelles.[22] D'après lui, cette approche porterait les individus à être plus attentifs à la gestion qui est faite de leurs données, de la même façon que les titulaires des droits d'auteur se préoccupent des usages qui sont faits de leur propriété intellectuelle.[23]

---

[21] C'est l'argument porté par Julie Cohen, qui critique le centralité du consentement comme outil permettant aux individus d'exercer leur autonomie, puisque le consentement est aujourd'hui obligatoire pour pouvoir accéder à tout service en ligne. Cohen, J. E. (2018). Turning Privacy Inside Out.

[22] Dans cet article, L. Lessig revendique qu'une approche patrimoniale à la protection des données personnelles permettrait de renforcer la force rhétorique qui sous-tend le droit à la protection de la vie privée (p. 247). Il précise, notamment, qu'une approche patrimoniale pour les données personnelles impliquerait que toute modification unilatérale des politiques de confidentialité (*privacy policy*) serait alors considéré non plus comme une simple atteinte à la vie privée des individus, mais comme un véritable "vol" des données (p. 255). Lessig, L. (2002). Privacy as property. *Social Research: An International Quarterly*, *69*(1), 247-269.

[23] L. Lessig considère que, s'ils détenaient des droits de propriétés sur leurs données personnelles, les individus seraient beaucoup plus attentifs à leur droits, et plus motivés à s'opposer à une utilisation non-autorisée de ces données (p. 250). Lessig, L. (2002). Privacy as property. *Social Research: An International Quarterly*, *69*(1), 247-269.

En France, certains juristes se prononcent aussi en faveur de cette approche patrimoniale. C'est le cas, notamment, d'Alain Bensoussan, qui a longtemps revendiqué que, dans un monde en hyper-connexion, caractérisé par la montée en puissance des big data, la monétisation des données personnelles deviendra tôt ou tard un phénomène incontournable, qui demandera un passage d'un droit à la protection vers un droit à la propriété des données personnelles.[24] Il en va de même pour Isabelle Landreau, avocate au barreau de Paris, qui considère que puisque les données des citoyens génèrent un revenu indirect aux grands prestataires de services en ligne (les GAFA), ils devraient pouvoir récupérer un reversement proportionnel sous forme de nano-paiement pour l'exploitation de leurs données."[25]

Les arguments en faveur de cette approche patrimoniale sont fondés sur une approche libérale, qui prévoit que tout individu a le droit de disposer librement de ses ressources. Ainsi, le fait de conférer aux citoyens un droit de propriété sur les données les concernant reviendrait à leur donner le droit de monétiser leurs données personnelles, de la même façon que les auteurs peuvent commercialiser leurs œuvres. Étant donné les intérêts financiers qui y sont associés, les individus seront plus susceptibles de surveiller la façon dont ces données seront exploitées par des tiers.

Mais quelle serait donc la forme que prendrait ce droit patrimonial sur les données personnelles? Étant donné le caractère immatériel de ces données, il paraît naturel de se référer au régime de la propriété intellectuelle.

Aujourd'hui, dans le droit français, le régime de propriété intellectuelle ne protège que certaines catégories de ressources immatérielles, telles que les œuvres de l'esprit (droits d'auteur), les inventions (brevets), les marques, ou les secrets industriels. Ce régime reconnaît aussi un droit *sui generis* sur les bases de données, dans la mesure où celles-ci attestent d'un "investissement financier, matériel ou humain substantiel".[26] Or, ce droit ne porte en aucun cas sur les données brutes en tant que telles, mais uniquement sur la collecte ou la réutilisation répétée ou massive de ces données. Les données personnelles en tant que ressource incorporelles ne bénéficient donc d'aucun statut juridique dans le régime de droit existant.

Une approche patrimoniale nécessiterait alors d'une réforme juridique introduisant un nouveau droit de propriété (intellectuelle ou autre) sur les données personnelles. En février 2018, le député Bruno Bonnell, représentant du groupe La République en marche (LRM) à l'Assemblée Nationale, a déposé un amendement dans ce sens, dans le cadre du projet de loi relatif à la protection des données personnelles. Cet amendement proposait de reconnaître un nouveau droit de propriété intellectuelle sur les données personnelles pour permettre aux individus de monnayer les utilisations de ces données. Cette proposition a cependant été rejetée par l'Assemblée Nationale.

En effet, malgré la popularité grandissante de ces propositions, il existe aujourd'hui de nombreuses objections contre une approche patrimoniale à la protection des donnés

[24] A. Bensoussan, « Informatique et libertés », Ed. Francis Lefebvre, 2008, n°280 p.39.

[25] Isabelle Landreau dans le Rapport du think-tank Génération Libre: Mes Data sont à moi: pour une patrimonialité des données personnelles, Janvier 2018.

[26] Article L. 341-1 du code de la propriété intellectuelle

personnelles.[27] Pour la CNIL, il s'agit d'une "fausse bonne idée"[28] qui donnerait plus de pouvoir aux GAFA sur la manière dont il peuvent collecter et traiter les données personnelles des citoyens. En effet, en disposant du droit de propriété portant sur les donnés personnelles, les citoyens renonceraient alors à la possibilité de s'opposer à toute invasion de leur vie privée découlant du traitement ou de l'utilisation de ces données. Les GAFA bénéficieraient alors d'un contrôle absolu sur l'exploitation des données personnelles dont ils sont devenus titulaires. Le Conseil National du Numérique a, lui aussi, récemment publié un rapport soulignant les problèmes inhérents à cette approche. Le rapport fait référence non seulement à la difficulté d'établir la portée de ce qui constitue effectivement une donnée personnelle (dont la définition s'élargit de jour en jour), mais aussi à l'incertitude concernant la titularisation de ces données - surtout lorsque celles-ci ont été générées par des analyses statistiques et des algorithmes d'apprentissage automatique.[29]

Le droit doit s'efforcer d'équilibrer les intérêts personnels des citoyens et le respect de leurs droits et libertés fondamentales, avec les intérêts patrimoniaux de ces mêmes individus - ainsi que ceux des opérateurs responsables du traitement. Une solution qui permettrait peut-être de réconcilier l'approche patrimoniale avec le droit personnel sur la protection des données serait d'accompagner le droit de propriété sur les données personnelles avec des droits extra-patrimoniaux. Comme avec le droit d'auteur, où les auteurs disposent aussi bien de droits exclusifs (dont ils peuvent disposer librement) et de droits moraux (qui sont, eux, inaliénables), il serait possible de mettre en place un régime de protection hybride, comprenant aussi bien des droits patrimoniaux que des droits extra-patrimoniaux. Alors que les premiers porterait sur la collecte, le traitement, et l'exploitation commerciale des données, les seconds porterait sur des droits liés à la dignité des individus, tels que le droit d'accès, de portabilité, de rectification, ou encore, le droit à l'oubli.

Mais au-delà des difficultés liées à la mise en place de cette approche, il existe aussi une objection de nature plus idéologique ou éthique. Le droit européen doit-il évoluer dans une direction qui privilégierait la commercialisation, plutôt que la protection des données personnelles? Cette approche patrimoniale est-elle capable de mieux répondre aux besoins des citoyens, et de mieux protéger leurs intérêts individuels? S'il est possible que, dans le court terme, monnayer les données personnelles permettrait aux citoyens de partager une partie des profits générés par les GAFA, cela ne conduirait-il pas à une dénaturation de ces droits fondamentaux auxquels appartient la protection de la vie privée? En particulier dans le cas des données de santé, qui représentent les aspects les plus intimes de l'homme, la monétisation de ces données ne comporterait-elle pas une violation de certaines prérogatives d'ordre public ? S'il est interdit de commercialiser certaines parties du corps humain, est-il acceptable de

[27] Anciaux, A., & Farchy, J. (2015). "Données personnelles et droit de propriété: quatre chantiers et un enterrement" *Revue internationale de droit économique*, 29(3), 307-331.

[28] CNIL, «Vie privée à l'horizon 2020. Paroles d'experts», *Cahiers IP Innovation et prospective*, n° 1.

[29] Avis du Conseil National du Numérique sur "La libre circulation des données dans l'union Européenne", Avril 2017.

commercialiser les données qui représentent des informations émanant du corps humain? N'y aurait-il pas là un risque de créer une situation d'inégalité, où les citoyens les plus pauvres seraient encouragés à disposer de leurs données personnelles pour accéder à un service gratuitement, et où seuls les citoyens les plus riches pourraient alors se permettre d'avoir leur vie privée respectée? Enfin, qu'en est-il de la révocabilité de ces actions? Alors que, dans le cadre juridique actuel, le consentement peut être révoqué à tout moment, dans l'optique patrimoniale, après avoir disposé de leurs droits, les individus n'auraient plus la possibilité de reprendre le contrôle sur leurs données personnelles, même si leur exploitation s'avère aller à l'encontre de leur dignité.

Si le droit actuel sur la protection des données personnelles est incapable de garantir une protection effective de la vie privée - car un consentement généralisé est souvent demandé pour accéder à tout service en ligne -, le fait de conférer des droits de propriété sur les données personnelles présente aussi de grands inconvénients. Alors qu'une situation de ce genre n'est pas susceptible de promouvoir l'intérêt général, elle est d'autant plus problématique dans le cas des données de santé qui représentent des données sensibles méritant un niveau de protection plus élevé.

IV- Conclusion: Vers un droit collectif sur un bien commun de données de santé

Le droit doit trouver un moyen de protéger les intérêts privés des individus- d'autant plus qu'ils participent volontairement à cette collecte par des techniques de plus en plus sophistiquées de "la mesure de soi"- sans pour autant porter atteinte aux prérogatives d'intérêt général que l'État défend. Sur ce point, il est utile de s'interroger sur la nature individuelle et collective du droit au respect de la vie privée. D'une part, il s'agit d'un droit afférant à l'intimité de la personne—un droit de nature donc profondément individuel. D'autre part, cependant, le droit à la vie privée a acquis une nouvelle signification avec l'arrivée des technologies numérique et de l'Internet. Initialement perçu comme un droit visant à limiter les interférences au sein de la sphère privée des individus, le droit au respect de la vie privée s'est progressivement décliné en plusieurs sous-catégories de droits, y compris le droit sur la confidentialité des communications et sur la protection des données personnelles. Aujourd'hui, ces droits se manifestent pour la plupart dans une optique relationnelle: si un individu communique avec un autre individu qui ne protège pas la confidentialité de ses communications, il sera impossible pour le premier individu de maintenir le contrôle sur les informations communiquées le concernant. Ainsi, dans un monde hyper-connecté, le droit à la vie privé ne peut plus être perçu uniquement comme un droit

individuel, mais doit aussi être interprété comme un droit collectif - un droit qui se rapporte aux individus, mais qui peut (oui qui doit) être exercé en commun ou de manière collective.[30]

Les données, comme nous l'avons dit plus haut, ne sont plus des données personnelles, mais des "données en réseaux" qui lient plusieurs personnes les unes avec les autres. Dans une société hyperconnecté, où nous interagissons constamment les uns avec les autres, il est de plus en plus difficile d'identifier des données qui sont vraiment "personnelles" (i.e. afférentes à une personne). Désormais, les données sont non plus seulement interconnectées, mais aussi interdépendantes: elles se renseignent mutuellement pour créer un jeu de données personnelles et collectives. Par exemple, la carnet d'adresse d'une personne contient des données sensibles, pas seulement par rapport au titulaire de ce carnet d'adresse, mais aussi par rapport à chaque individu présent au sein de ce carnet. Ces données "personnelles" ne peuvent donc pas être isolées ou associés à un seul individu concerné. Même dans le cas de données personnelles non interconnecté, la donnée personnelle d'un individu pourraient aussi révéler des informations personnelles concernant un autre individus (notamment, dans le cas du génome humain). Par consentement, un individu autorisant la collecte ou le traitement de ses données personnelles empièterait alors sur le droit à la vie privée d'autres individus.

C'est ainsi qu'il est difficile de justifier l'introduction d'un droit de propriété individuel sur ces données, qui n'appartiennent à personne et à tout le monde en même temps. De même, une logique orientée exclusivement sur un droit personnel ne fait pas sens, puisque cela accorderait à des individus le droit de céder ou de consentir au traitement de données sensibles, qui dévoilent aussi des informations personnelles sur autrui. Nous rejoignons en cela Pierre Bellanger qui, après avoir défendu la patrimonialité des données personnelles,[31] est revenu sur une position défendant le droit à la protection de la vie privée. D'après lui, les données personnelles ne peuvent pas faire objet d'un droit de propriété ni d'un droit personnel ou individuel. Ces données en réseau, afférentes à plusieurs individus, devrait plutôt être regardées comme un "bien commun" dont la protection, à cause de certains missions d'intéret général poursuivies doit être assurée par l'état.

Une conception plus collective du droit au respect de la vie privée a aussi été récemment proposée par Julien Cohen dans son article "Turning Privacy Inside Out",[32] où l'auteur considère que la vision individualiste du droit à la protection des données personnelles est insuffisante à garantir le respect de la vie privée sur Internet. Elle propose alors d'adopter une optique plus paternaliste, où l'Etat est responsable pour garantir une protection suffisante de la vie privée, non pas en conférant des droits aux individus, mais en introduisant des contraintes sur la façon dont

[30] Pour une explication plus détaillé de la distinction entre droits individuels et droits collectifs, voir G. Koubi (2008) "Distinguer entre droits individuels et droits collectifs", disponible sur https://koubi.fr/spip.php?article13
[31] Bellanger, P. (2014). *La souveraineté numérique*. Stock.
[32] Cohen, Julie E., Turning Privacy Inside Out (April 12, 2018). Theoretical Inquiries in Law 20.1 (2019 Forthcoming). Available at SSRN: https://ssrn.com/abstract=3162178

les opérateurs peuvent collecter ou traiter les données personnelles, indépendamment du consentement des personnes concernées. Le fait de considérer le droit au respect de la vie privée comme un droit collectif plutôt qu'un droit individuel permettrait alors à tout individu de s'opposer aux utilisations illégitimes qui sont faites des données personnelles de soi ou d'autrui, afin de s'assurer que l'intérêt général soit respecté et que la dignité humaine soit elle-même préservée.

Aussi bien l'approche proposée par Pierre Bellanger, que la vision de Julie Cohen comportent une conception de la vie privée comme un "bien collectif" ou "bien commun" qui doit être donc protégé par l'État au même titre que la santé ou l'éducation. En ce sens, les données personnelles et, en particulier, des données de santé, ne peuvent pas être protégées avec une approche libérale concentrée sur la maximization des libertés individuelles (par le biais du consentement ou de la patrimonialisation de ces données) mais il serait plutôt nécessaire d'adopter une optique plus communautaire ou collective, qui pourrait exiger une limitation de certaines libertés individuelles, au nom de l'intérêt général et du bien commun.

_____