Editorial

La recherche sur le dossier médical informatisé a eu un essor très important jusqu'à la fin du siècle dernier. Les solutions logicielles sont largement diffusées à présent et les cabinets médicaux équipés. Les données médicales sont donc éclatées entre les différents lieux de soins sans faciles possibilités de partage ou de transmission aux patients.

A cela, aujourd'hui, s'ajoutent de nouvelles pratiques liées à l'essor des nouvelles technologies : photographie d'un résultat d'analyse avec un téléphone portable (personnel ou professionnel), flux d'échanges d'ordonnances ou de résultats médicaux par mail, utilisation d'appareils connectés (IRM, scanners de tomographie, etc.), dispositifs médicaux pour différents usages (pilulier connecté par exemple), suivi à distance des paramètres médicaux patients. En substance, les pratiques changent de la part des soignants et des patients, intégrant de plus en plus souvent, les appareils personnels dans la collecte de données de santé.

Ces nouveaux dispositifs associés à des usages moins contraints et plus puissants de collecte et d'échange de données de santé dénormalisent les pratiques usuelles. Ils augmentent le risque d'interception de ces données dans les réseaux (failles de sécurité de l'IoT par exemple) et leur dispersion. Les patients sont de plus en plus exclus de la maîtrise de leurs données de santé, reconstruire leur histoire santé se complexifie également et malgré un règlement européen[1] contraignant, n'ont pratiquement aucune possibilité de savoir qui utilise leurs données de santé ni à quelles fins.

A la nécessité de « redonner le pouvoir » aux patients sur ses données afin qu'il devienne un **patient souverain**, s'ajoute toutefois une approche qui pourrait paraître contradictoire sur une tendance actuelle de **de réutilisation des données** pour alimenter des systèmes d'IA (bien souvent sans le consentement du patient).

Des recherches sont déjà menées dans le domaine. Quelques exemples suivent.

Agent (ou patient) souverain : blockchain et self-sovereign identity

Dans (Houtan *et al.*, 2020), les auteurs s'intéressent à la convergence de l'identité physique et numérique et l'intégration de divers dossiers individuels, tels que les données des patients, dans un référentiel unifié. Ils abordent l'antagonisme entre la collecte de données pertinentes pour aider les cliniciens, les spécialistes et les prestataires de services de santé à faciliter la prise en charge des patients et le droit, pour les patients, de contrôler leurs données personnelles, droit qui est remis en question, car les patients ne manipulent pas leurs données de manière explicite. Ils font un état de l'art en matière d'autosouveraineté basée sur la blockchain (BC) et d'enregistrement des données des patients dans le domaine des soins de santé. Ils partent de l'hypothèse que la technologie des grands livres distribués (DLT) est une nouvelle méthode qui permettrait d'enregistrer en toute sécurité des données horodatées et de mettre en place des dossiers de santé et d'identité pilotés par les patients.

Il ne s'agit pas de faire du prosélytisme de blockchain pour des usages sociétaux aussi sensibles que ceux touchant à l'identité ou à la santé. La technologie appliquée à des domaines où ses caractéristiques ne sont pas mobilisées perd sa pertinence. Il est alors préférable d'opérer le service depuis une base de données centralisée, ou décentralisée, voire distribuée (comme Storj) ou de simple registre distribué fermé ou ouvert (Ripple et Corda). Conscient de l'impact environnemental de la solution technique choisie, il est important de plébisciter celle qui présente le meilleur potentiel pour le moins d'incidence. La blockchain publique présente un intérêt si l'on cherche la

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

conservation sécurisée des données/transactions, assurer l'immutabilité des données/transactions et surtout, grâce à son caractère distribué la possibilité d'adresser simultanément plusieurs informations. Dès lors, les services rendus par la blockchain peuvent être résumés ainsi une solution distribuée facilitant et améliorant la procédure de vérification - identification et authentification - par l'utilisateur/patient ou par une personne morale, pour l'accès et l'obtention de services ou pour la fourniture de preuves numériques à toutes fins utiles en matière de santé.

Le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit eIDAS[2]), a pour objectif d'assurer l'interopérabilité des systèmes d'identification et d'authentification des solutions d'identité numérique. Cette interopérabilité passe par une classification des moyens de mise en œuvre de différents niveaux de garantie (faible, substantiel et élevé). Il est envisagé une révision du règlement eIDAS qui permettra d'introduire certains services de confiances, tels que l'archivage électronique ou des technologies comme la blockchain, impliquant d'adapter «l'horodatage électronique sécurisé». Les informations relatives à l'identité relèvent, pour une grande partie, de l'article 5 du RGPD[3] qui implique que les données à caractère personnel doivent être a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence); b) collectées pour des finalités déterminées, explicites et légitimes (limitation des finalités); c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données); d) exactes et, si nécessaire, tenues à jour (exactitude); e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (limitation de la conservation); f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel (intégrité et confidentialité).

Dans (Hummel *et al*., 2021), les auteurs abordent la confrontation des agents à la difficulté de garder le contrôle de leurs données. Leur méta-analyse a pour but d'analyser la fréquence de différentes notions telles que la souveraineté des données, la souveraineté numérique et la cybersouveraineté dans des contextes problématiques. Les auteurs constatent que le concept de souveraineté des données fait allusion à un mélange nuancé de concepts normatifs tels que la délibération inclusive et la reconnaissance des droits fondamentaux des personnes concernées par les données.

La « Self sovereign identity » est un concept qui désigne la possibilité pour les personnes physiques d'héberger et de gérer les éléments de leur identité, grâce à des dispositifs personnels ou en ligne. Dit autrement, les individus ont, grâce aux outils technologiques de type blockchain, la maîtrise de leur identité numérisée, sans organe centralisateur. Cette solution peut être déclinée en matière de santé, « self sovereign health ». La souveraineté technologique des individus ne questionne pas la souveraineté régalienne, l'Etat reste le garant de l'identité juridique ou la gestion de la santé publique. Maîtres de ces attributs, les individus peuvent alors en avoir une utilisation frugale, en choisissant de ne divulguer que les données absolument nécessaires au service attendu.

Ce concept d'identité autosouveraine ou de santé autosouveraine s'inscrit dans la continuité d'un principe plus ancien, celui de l'autodétermination informationnelle. De nombreux travaux ont été consacrés à l'autodétermination informationnelle. Elle est issue du droit allemand. La loi fédérale du 20 décembre 1990 sur la protection des données, modifiée ultérieurement, a remplacé la loi du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle

---

[2] Règlement (UE) No 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données

dans le cadre du traitement des données. Avec la loi fédérale de 1977, l'Allemagne avait été le premier pays à se doter d'un texte général sur la protection des données personnelles. L'abrogation de la loi de 1977 fut notamment la conséquence de l'arrêt rendu par la Cour constitutionnelle en 1983 sur la loi relative au recensement de la population. La Cour constitutionnelle dégagea en effet à cette occasion un nouveau droit constitutionnel : le droit à " l'autodétermination informationnelle ", c'est-à-dire le droit pour chaque individu de décider lui-même de la communication et de l'emploi des informations le concernant. Des auteurs reconnus du CRID en Belgique ont travaillé sur cette notion (Rouvroy et Poullet, 2009) et (De Terwangne, 2015). Ce principe trouve une consécration dans la loi pour une République numérique (loi n° 2016-1321 du 7 octobre 2016, pour une République Numérique), qui a affirmé le droit pour tout individu à la libre disposition de ses données en complétant l'article premier de la loi Informatique et libertés d'un alinéa qui dispose : «Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi ». Ce qui distingue donc la Self Sovereign Identity de l'autodétermination informationnelle, c'est que la première octroie une maîtrise technologique aux individus sur les attributs de leurs identités, alors que la seconde leur assure une maîtrise juridique.

Utilisation des données de santé

Dans (Xia *et al.*, 2017), les auteurs ont créé le système MeDShare qui aborde la question du partage des données médicales entre les dépositaires de big data médicaux dans un environnement sans confiance. Le système est basé sur la blockchain et fournit la provenance des données, l'audit et le contrôle des données médicales partagées dans des référentiels en nuage entre les entités de big data.

Dans (Murphy *et al.*, 2021), les auteurs abordent le fonctionnement des référentiels de données biomédicales sous l'angle des efforts déployés pour améliorer la manière dont les données scientifiques sont traitées et mises à disposition sur le long terme. Ils notent que de nombreux groupes ont formulé des recommandations sur les fonctions que les dépôts de données biomédicales devraient prendre en charge, et beaucoup utilisent les exigences des principes de données FAIR comme lignes directrices. Les auteurs constatent que FAIR n'est qu'un ensemble de principes issus de la communauté de la science ouverte qui sont rejoints par des principes régissant la science ouverte, la citation des données et la fiabilité, qui sont tous des aspects importants à prendre en charge par les dépôts de données biomédicales. Ensemble, ils définissent un cadre pour les dépôts de données que les auteurs nomment OFCT : Open, FAIR, Citable and Trustworthy. Ils ont développé un instrument à code source ouvert qui tente d'opérationnaliser les aspects clés des principes OFCT.

Dans une problématique connexe, des auteurs s'intéressent à la blockchain en santé. Dans (Agbo *et al.*, 2019), les auteurs présentent un examen systématique des recherches en cours sur l'application de la technologie blockchain dans les soins de santé. La méthodologie de recherche est basée sur les directives PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) et sur un processus d'étude systématique de cartographie, dans lequel un protocole de recherche bien conçu est utilisé pour interroger quatre bases de données scientifiques, afin d'identifier, d'extraire et d'analyser toutes les publications pertinentes. Leur constat est qu'un certain nombre d'études ont proposé différents cas d'utilisation pour l'application de la blockchain dans les soins de santé ; cependant, il y a un manque de mises en œuvre de prototypes adéquats et d'études pour caractériser l'efficacité de ces cas d'utilisation proposés.

Le projet MyHealth MyData (MHMD[4]) a pour but de sécuriser les données des patients, de réduire le risque d'usurpation d'identité et de violation de la vie privée (*privacy by design*), et d'introduire une nouvelle façon de partager les informations privées en responsabilisant leurs

[4] http://www.myhealthmydata.eu/why-mhmd/

principaux propriétaires, les patients. Le projet est basé sur des technologies : blockchain, calcul sécurisé, apprentissage distribué et données synthétiques (obtenues à partir de données synthétisées).

Le Health Data Hub a pour but de créer une plateforme de données de santé partagées pour accélérer la recherche scientifique. L'hébergement des données confié à Microsoft a d'ailleurs soulevé la polémique (https://www.esante.tech/les-polemiques-soulevees-par-le-health-data-hub/).

La Commission européenne a présenté sa stratégie pour « façonner l'avenir numérique de l'Europe », s'inscrivant dans une « décennie du numérique » et affirmant « une société européenne soutenue par des solutions numériques qui placent les citoyens au premier plan, ouvrent de nouvelles perspectives aux entreprises et encouragent le développement de technologies fiables pour promouvoir une société ouverte et démocratique et une économie dynamique et durable[5] ». La mise en place de Mon Espace Santé du gouvernement (https://www.monespacesante.fr/) accroît également ce glissement vers le « tout numérique » en santé.

Ce numéro spécial de la revue ouverte d'ingénierie des systèmes d'information a pour but de croiser les regards pluri- ou inter-disciplinaires sur la question du patient souverain.

L'article de Doriane Pérard aborde la problématique du suivi hors les murs de l'hôpital des patients porteurs de bactéries hautement résistantes aux antibiotiques. Ces bactéries représentent un challenge de santé publique majeur pour les décennies à venir et dont les observateurs ne masquent pas la dangerosité. Elle présente une solution technologique basée sur une blockchain privée pour résoudre le stockage et le partage de données chaînées par des procédés cryptographiques. Au travers de son article, l'autrice cherche à résoudre un conflit inhérent aux blockchains : une philosophie basée sur une absence de médiation centralisée du contrôle des données et la nécessité de protéger les données de santé via le RGPD.

L'article d'Aurélie Bayle et Gwenaëlle Donadieu interroge la notion juridique de consentement éclairé du patient au regard des sciences comportementales. Elles notent le glissement d'une médecine du secret à une médecine du partage et l'ambivalence qui peut émerger d'un accroissement du besoin de protéger les données de santé en regard de la nécessité pour le patient de diffuser plus d'informations sur lui-même. Les autrices se posent alors la question de la pertinence d'utiliser les apports des sciences comportementales dans le contexte du traitement de données à caractère personnel de santé.

Nous remercions les autrices pour leurs contributions à ce numéro spécial ainsi que les membres du comité de lecture pour leur participation à la relecture des articles.

Christine Verdier & Amélie Favreau

Agbo C.C., Mhamoud Q.H., Eklund J.M. (2019). *Blockchain Technology in Healthcare: A Systematic Review*. Healthcare (Basel), 2019-04-04, Vol.7 (2). DOI: 10.3390/healthcare7020056

Allen C. (2018). *Forging self-sovereign identities in the age of the Blockchain*. Conférence Rebooting the Web of Trust, Nov 2018, en ligne, https://bitcoin.fr/christopher-allen-*Blockchain*et-identite-video/

Coutor S., Hennebert C., Mourad F. (2021). *Blockchain et identification numérique*. Restitution des ateliers du groupe de travail « Blockchain et identité » (BCID), Ministère de l'Intérieur, 2021.

De Terwangne, C. (2015). *Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ?*. Dans Le droit à l'oubli numérique : données normatives - approche comparée (p. 23-50). (Création Information Communication). Larcier. http://www.crid.be/pdf/public/7684.pdf)

[5] Communiqué de presse : https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_273

Houtan B., Abdelhakim S., Makrakis D. (2020). *A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare*. IEEE access, 2020, Vol.8, p.90478-90494. DOI: 10.1109/ACCESS.2020.2994090

Hummel P., Braun M., Tretter M., Dabrok P. (2021). *Data sovereignty: A review*. Big data & society, 2021-01, Vol.8 (1). https:// doi.org/10.1177/2053951720982012

Murphy F., Bar-Sinai M., Matrone M.E., Naudet F. (2021). *A tool for assessing alignment of biomedical data repositories with open, FAIR, citation and trustworthy principles*. PloS one, 2021-07-09, Vol.16 (7), p.e0253538-e0253538. DOI: 10.1371/journal.pone.0253538

Rouvroy A., Poullet Y. (2009). *Le droit à l'autodétermination informationnelle et la valeur du développement personnel: une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie*. Dans K. Benyekhlef, & P. Trudel. (eds.), Etat de droit et virtualité (p. 157-222). Thémis.

Wang F. De Filippi P. (2020). *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*. Frontiers in Blockchain. 2-28. DOI:10.3389/fbloc.2019.00028

Xia Q., Sifah E.B., Asamoah K.O., Gao J., Du X., Guizani M. (2017). *MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain*. IEEE access, 2017, Vol.5, p.14757-14767. DOI: 10.1109/ACCESS.2017.2730843

Relecteurs

Mehdi AMMI, Université Paris 8
Guillaume CABANAC, Université Toulouse 3 Paul Sabatier, IRIT
Jérôme DARMONT, Université Lyon 2
Rebecca DENECKERE, Université Paris 1 Panthéon-Sorbonne
Agnès FRONT, Université Grenoble Alpes
Caroline LE GOFFIC, Université de Lille
Jessica EYNARD, Université Toulouse 1 Capitole
Mohamed Ali KANDI, Université Toulouse 3 Paul Sabatier