Universités de Fribourg, Genève,
Lausanne et Neuchâtel

Programme doctoral romand de droit

Le droit face à la révolution 4.0

Édité par

Jean-Philippe Dunand
Anne-Sylvie Dupont
Pascal Mahon

Avec la collaboration de
Xenia Karametaxas et Jean Perrenoud

Schulthess
ÉDITIONS ROMANDES

Universités de Fribourg, Genève,
Lausanne et Neuchâtel

Programme doctoral romand de droit

Le droit face à la révolution 4.0

Édité par

Jean-Philippe Dunand, professeur
Anne-Sylvie Dupont, professeure
Pascal Mahon, professeur

Avec la collaboration de
Xenia Karametaxas et Jean Perrenoud

Schulthess § 2019
ÉDITIONS ROMANDES

Citation suggérée de l'ouvrage : Jean-Philippe Dunand / Anne-Sylvie Dupont / Pascal Mahon (éds), *Le droit face à la révolution 4.0*, collection CUSO, Genève/Zurich 2019, Schulthess Éditions Romandes

Publié avec l'aide de la Conférence universitaire de Suisse occidentale

ISBN 978-3-7255-8717-9

www.schulthess.com

Diffusion en France : Lextenso Éditions, 70, rue du Gouverneur Général Éboué, 92131 Issy-les-Moulineaux Cedex
www.lextenso-editions.com

Diffusion et distribution en Belgique et au Luxembourg : Patrimoine SPRL, Avenue Milcamps 119, B-1030 Bruxelles ; téléphone et télécopieur : +32 (0)2 736 68 47 ; courriel : patrimoine@telenet.be

Information bibliographique de la Deutsche Nationalbibliothek :
La Deutsche Nationalbibliothek a répertorié cette publication dans la Deutsche Nationalbibliografie ; les données bibliographiques détaillées peuvent être consultées sur Internet à l'adresse http://dnb.d-nb.de.

Sommaire

Blockchain et santé : perspectives juridiques en Suisse

par

FRÉDÉRIC ERARD[1]

Introduction

Le champ d'application de la technologie *blockchain* ne se limite pas aux cryptomonnaies. En procurant un registre décentralisé et distribué (et donc sans autorité centrale), transparent, sécurisé, infalsifiable et historisé, les *blockchains* peuvent être utilisées pour la tenue de registres publics, pour l'enregistrement des droits d'auteurs ou pour la traçabilité des produits alimentaires. La santé n'est pas oubliée. En Amérique du Nord et en Asie, des propositions ont été avancées pour asseoir la gestion des dossiers médicaux sur la technologie *blockchain*. Deux intérêts en apparence inconciliables pourraient alors converger : renforcer la protection des données de santé en offrant

[1] Les recherches menées à l'appui du présent article ont été réalisées en grande partie lors d'un séjour de recherche doctorale d'une année à l'Université de McGill, Montréal, rendu possible grâce à une bourse Doc.Mobility du Fonds national suisse de la recherche scientifique (FNS). L'auteur tient ici à témoigner sa gratitude envers le FNS et l'Université de McGill.

au patient un meilleur contrôle sur celles-ci et permettre aux tiers intéressés (autres soignants, recherche, etc.) d'accéder plus facilement aux données de santé des patients.

La présente contribution s'articule en quatre parties : la première partie aborde le contexte général des pressions exercées aujourd'hui sur les données de santé. La deuxième partie esquisse les caractéristiques générales de la technologie *blockchain*. La troisième partie présente les caractéristiques générales des modèles *blockchain* de gestion des dossiers médicaux et aborde une sélection de questions juridiques suscitées par cette thématique. Enfin, la quatrième partie offre un aperçu d'autres applications possibles de la technologie *blockchain* dans le secteur de la santé.

La technologie *blockchain* est encore émergente et ses évolutions rapides. Menées dans une optique essentiellement prospective, les réflexions qui suivent tendent davantage à identifier les problématiques juridiques posées qu'à leur donner des réponses juridiques claires, impossibles à fournir en l'absence d'un objet d'étude précisément arrêté.

I. Données personnelles de santé et intermédiaires

Examiné sous l'angle historique, le secret médical est un concept particulièrement malléable dont l'application plus ou moins stricte a été influencée selon les époques par une pluralité de facteurs (social, économique, politique, médical, historique, etc.)[2]. Cette affirmation peut être transposée au contexte plus large et plus récent de la protection des données personnelles de santé. Au cours des dernières décennies, plusieurs facteurs ont contribué à augmenter sensiblement le nombre de communications de données personnelles de santé, notamment :

- le rôle interventionniste croissant de l'État et l'augmentation du nombre d'exceptions légales au secret médical, y compris à des fins de surveillance épidémiologique ;

- l'exercice de la médecine dont l'évolution implique une augmentation du nombre et du type de soignants (spécialisations, équipes de soins, interprofessionnalité, réseaux de soins…) ;

- les pressions économiques visant à mieux contrôler les coûts de la santé ;

- l'évolution des besoins médicaux de la population, notamment en lien avec la démographie et l'augmentation du nombre de maladies chroniques. Les nouveaux modèles de fourniture de soins développés pour répondre à ces défis (ex. : soins intégrés) impliquent un besoin accru de communications sur le long terme ;

- l'avènement de l'informatique et ses différentes ramifications (cloud, dossier électronique du patient…) qui implique une multiplication des lieux de stockage et facilite l'accès aux données ainsi que leurs échanges ;

[2] Voir notamment : RIEDER/LOUIS-COURVOISIER/HUBER, p. 153.

- les nouvelles technologies médicales dont le fonctionnement nécessite un large accès aux données de santé des patients (*Big Data*, intelligence artificielle, médecine de précision) ;

- la recherche biomédicale dont les avancées requièrent un accès toujours plus large aux données personnelles de santé.

L'augmentation des échanges de données s'accompagne d'une multiplication des détenteurs de données, qu'il s'agisse d'établissements de soins, de professionnels de la santé, de sous-traitants, d'organismes étatiques, d'assureurs ou de centres de recherche. Tous ces acteurs agissent comme des *intermédiaires* potentiels dans la gestion de ces données. L'individu qui entend faire valoir ses droits doit alors généralement traiter individuellement avec chacun des intermédiaires.

Les intermédiaires ont rarement une vision complète des données de santé relatives à un patient ou à un sujet de recherche. Ces dernières sont fragmentées et disséminées entre les différents acteurs du système de santé. Le patient lui-même est souvent incapable de désigner avec exactitude quels intermédiaires détiennent des informations le concernant, ni dans quelle étendue. Ainsi, à mesure que le nombre d'intermédiaires augmente, le contrôle de l'individu sur ses propres données diminue. D'autre part, même s'il est justifié, l'accès aux données de santé par des tiers est lui aussi entravé par la fragmentation du stockage des données de santé (on parle parfois de « silos » d'information[3]). Cette situation entraîne non seulement une augmentation des coûts de la santé (ex. : examens médicaux à double), mais elle entre en contradiction avec les nouveaux modèles de soins qui impliquent des collaborations interprofessionnelles étroites sur le long terme. Elle empêche aussi un accès approprié aux données à des fins de recherche biomédicale ou le développement de nouvelles formes de médecine basées sur le *Big Data* et l'intelligence artificielle. Enfin, l'informatisation de la gestion des données de santé et les nombreuses communications de données exposent inévitablement les données de santé à des risques de piratage et d'accès indus plus élevés que par le passé. Elles exposent à tout le moins des volumes de données plus importants à ces risques.

Pour répondre aux problématiques décrites ci-dessus, plusieurs initiatives aussi bien publiques que privées ont été lancées pour gérer les données de santé en recourant à la technologie *blockchain*. Avant d'en offrir un survol, il est nécessaire d'examiner les caractéristiques principales de cette technologie.

II. Technologie *blockchain*

La technologie *blockchain* – qu'on pourrait traduire par « *chaîne de blocs* » – est récente, évolutive, polymorphe et ne répond pour l'heure à aucune définition qui fasse consensus. Ses premières applications ont été développées pour la création de monnaie virtuelle (Bitcoin), mais son champ

[3] IVAN, p. 4 ; MCFARLANE, p. 2.

d'application potentiel est bien plus large[4]. Les développements qui suivent se limitent à présenter les caractéristiques générales de cette technologie avec un accent particulier sur les aspects les plus pertinents pour la présente analyse juridique.

La *blockchain* est un registre d'informations ou de transactions *peer-to-peer* (« P2P ») qui a pour objet un historique distribué dans une structure décentralisée[5]. L'information enregistrée sur la *blockchain* est détenue par l'ensemble des nœuds informatiques (« *nodes* ») qui composent le réseau et qui participent au fonctionnement de la *blockchain*. Ces nœuds possèdent une copie locale complète du registre[6], c'est-à-dire une copie de l'ensemble des blocs d'informations qui composent la *blockchain*[7].

Pour qu'une nouvelle information ou transaction soit enregistrée sur la *blockchain*, elle doit être insérée dans un *bloc* qui rassemble un groupe d'informations. La validation de chaque nouveau bloc doit être approuvée par les nœuds informatiques du réseau par le biais d'un système de consensus[8]. Le nouveau bloc est alors horodaté et lié mathématiquement à la chaîne des blocs précédents. L'ensemble des nœuds informatiques prennent individuellement en compte l'opération et complètent leur copie locale en conséquence.

Ce procédé a plusieurs conséquences, dont la plus significative est probablement le *caractère immuable des blockchains*[9]. Les informations ou les transactions qui y sont enregistrées sont en effet permanentes, irréversibles et donc infalsifiables. La modification d'un bloc d'information impliquerait la suppression de tous les blocs enregistrés subséquemment, opération qui nécessiterait le consensus d'une majorité des acteurs du réseau et qui réduirait à néant la fonctionnalité de la *blockchain*. Un acteur isolé ne peut donc pas modifier unilatéralement une information enregistrée sur la *blockchain*.

Comme la propriété, la gestion et le contrôle du registre incombent au réseau lui-même, les *blockchains* se caractérisent par l'*absence de toute autorité centrale*[10]. L'ensemble des informations ou des transactions enregistrées sur le réseau sont consultables en tout temps par l'ensemble des membres du réseau, voire par le grand public dans le cas des *blockchains* publiques (ex. : Bitcoin). La *blockchain* se caractérise donc par une *transparence* accrue, à tout le moins pour les acteurs du réseau[11].

Dans leur forme la plus courante, les *blockchains* recourent à des méthodes cryptographiques (signatures électroniques, hachage) qui, en plus de voiler le contenu de l'information, assurent une double fonction[12]. La première vise à *authentifier* les individus qui agissent sur le réseau. La

4 METTLER, p. 1.
5 DÉZIEL, p. 75-77 ; STENGEL/AUS DER AU, p. 439-441.
6 À tous le moins une partie des nœuds appelés « full nodes ».
7 BERBERICH/STEINER, p. 422.
8 OULD YAHIA/PARADINAS, p. 11. Il existe plusieurs types de consensus, les plus répandus étant les consensus « *Proof of Work* » (PoW) et « *Proof of Stake* » (PoS).
9 STENGEL/AUS DER AU, p. 441.
10 IVAN, p. 3 ; OULD YAHIA/PARADINAS, p. 11.
11 STENGEL/AUS DER AU, p. 441.
12 Pour une explication détaillée de ces deux fonctions, voir : DÉZIEL, p. 78-81.

seconde permet d'assurer *l'intégrité et l'authenticité* des données échangées, en particulier pour garantir qu'elles n'ont pas été modifiées ou tronquées au cours d'une transaction.

En principe, chaque individu ou acteur agit sur le réseau sous couvert d'un *pseudonyme* qui prend la forme d'une suite de symboles ou de chiffres (clé publique). La structure décentralisée de la *blockchain* couplée au recours à la cryptographie confère une *sécurité* informatique importante aux transactions effectuées sur la *blockchain*.

La technologie *blockchain* permet la programmation de « *contrats intelligents* » ou « *smart contracts* ». Il ne s'agit pas de contrats au sens traditionnel, mais de codes ou de programmes informatiques enregistrables sur la *blockchain* qui automatisent l'exécution d'une opération à la réalisation de conditions ou d'événements prédéterminés[13]. Les membres du réseau peuvent ainsi interagir sans l'intervention d'intermédiaire[14]. Des « contrats intelligents » – dont l'intégrité est directement garantie par la *blockchain* – peuvent par exemple être programmés pour autoriser des échanges d'informations sécurisés à des conditions prédéterminées (ex. : un individu peut autoriser à l'avance certains destinataires à consulter des renseignements le concernant sur la *blockchain*).

Les *blockchains* peuvent être classées en trois catégories[15] :

les *blockchains* publiques sans permission (« *public permissionless blockchain* ») ;

les *blockchains* publiques avec permission (« *public permissioned blockchain* ») ;

les *blockchains* privées (« *private blockchain* »).

Une *blockchain* est publique lorsque n'importe quel individu ou entité peut consulter l'historique des transactions et initier des transactions (ex. : Bitcoin). Dans les systèmes privés, seul un cercle défini et connu d'individus ou d'entités est en mesure de lire le contenu de la *blockchain* ou de procéder à des transactions. Des consortiums privés ont par exemple mis sur pied des structures de *blockchains* privées dans le domaine des banques ou des assurances pour profiter des avantages de la *blockchain* sans dévoiler des informations au grand public[16].

La distinction entre *blockchain* publique avec permission et *blockchain* publique sans permission ne dépend pas de l'accès aux informations enregistrées sur la *blockchain*, mais du mécanisme de consensus permettant de valider l'inscription de nouveaux blocs. Dans une *blockchain* publique sans permission, n'importe qui peut participer à la validation des transactions. À l'inverse, dans les *blockchains* publiques avec permission, seuls des valideurs connus et autorisés sont en mesure d'approuver des transactions[17]. Une fois approuvées par les valideurs, les informations enregistrées sur la *blockchain* sont publiques.

Des réserves sont régulièrement émises à l'égard des *blockchains* privées au prétexte qu'elles ne revêtiraient pas les caractéristiques essentielles des *blockchains*. Il est vrai qu'en restreignant l'accès du système (lecture et transactions) à un nombre fermé d'acteurs, les *blockchains* privées

13 STENGEL/AUS DER AU, p. 448-449 ; DÉZIEL, p. 81 ; OULD YAHIA/PARADINAS, p. 11.
14 DÉZIEL, p. 81.
15 ISLER, N 5 ss.
16 ISLER, N 7.
17 STENGEL/AUS DER AU, p. 441.

présentent un degré de décentralisation plus faible et s'apparentent davantage à des bases de données partagées traditionnelles[18]. Les *blockchains* privées rendent cependant la modification d'un registre plus difficile ou assurent encore une meilleure sécurité et intégrité des données.

Les *blockchains* connaissent un certain nombre de limitations. Outre des problèmes de gouvernance et de réglementation, les *blockchains* sont à l'heure actuelle confrontées à des problèmes techniques de « *scalability* »[19] qui se traduisent essentiellement par des lenteurs aussi bien en lien avec l'insertion de nouvelles informations dans les blocs que pour atteindre le consensus nécessaire à leur enregistrement. Ces obstacles liés à l'aspect décentralisé des *blockchains* impliquent par ailleurs des capacités limitées en matière de volume de données stockables ainsi que des coûts élevés de fonctionnement[20]. Enfin, le stockage décentralisé et les processus les plus courants de validation nécessitent de grandes quantités d'énergie et leur impact sur l'environnement est particulièrement critiquable.

III. Gestion des dossiers médicaux

1. Concepts développés

L'émergence de la technologie *blockchain* a inspiré le développement de nouveaux modèles de gestion des données de santé. À première vue, la technologie *blockchain* présente en effet plusieurs qualités aptes à parer aux problématiques qui fragilisent aussi bien le pouvoir du patient sur ses données que l'accès efficace aux données de santé par des tiers (problématiques de fragmentation, sécurité, coordination et partage des données de santé ; cf. *supra* § I.).

À ce jour, le projet le plus emblématique de gestion des dossiers médicaux sur la base de la technologie *blockchain* est le modèle « *MedRec* », développé par une équipe du MIT[21]. Plusieurs autres modèles, parfois directement inspirés de « *MedRec* », ont été développés à l'échelle théorique du moins. Dans sa contribution sur les *blockchains*, le partage de renseignements personnels sur la santé et le droit à la vie privée au Canada, DÉZIEL[22] a par exemple analysé de manière détaillée – en plus du modèle MedRec – trois autres modèles nord-américains développés respectivement par LINN/KOO[23], MCFARLANE (modèle « *Patientory* »)[24] et PETERSON ET AL. de la clinique Mayo[25]. Le modèle « *Ancile* » développé par DAGHER ET AL. paraît également digne d'être cité à côté de ces

[18] ISLER, N 13.
[19] KUO/KIM/OHNO-MACHADO, p. 1217; OULD YAHIA/PARADINAS, p. 12.
[20] DAGHER *et al*., p. 285.
[21] AZARIA *et al.,* p. 25 ss. Pour les développements subséquents du projet, consulter : <https://medrec.media.mit.edu>.
[22] DEZIEL, p. 82.
[23] LINN/KOO.
[24] MCFARLANE.
[25] PETERSON *et al.*

propositions[26]. Aux États-Unis, plusieurs concours publics et privés de projets d'application de la technologie *blockchain* au domaine de la santé ont été lancés au cours des dernières années, dont une compétition organisée par le gouvernement américain en 2016 au terme de laquelle quinze projets ont été primés[27]. L'Asie n'est pas non plus en reste avec un nombre important de projets similaires[28]. Sans faire la liste complète des initiatives en cours[29], il y a lieu de constater dans ce secteur l'existence d'une activité académique, industrielle et étatique croissante sur le plan international. En Europe, la recherche la plus notoire en la matière est le projet Horizon2020 « *My Health My Data* », actuellement mené par un consortium d'acteurs privés et publics à travers le continent et financé par la Commission européenne[30]. Ce projet vise à explorer la possibilité d'établir un cadre « *blockchain* » pour la gestion des données de santé en poursuivant le triple objectif de renforcer les droits individuels des patients, de garantir la protection des données des patients et d'augmenter la valeur des données de santé en rendant leur exploitation plus efficace. En Suisse, des chercheurs de l'EPFL et de la HES-SO travaillent en collaboration avec des chercheurs américains sur un système *blockchain* de partage de données en lien avec le traitement du cancer[31]. La startup zougoise « *healthbank* » propose par ailleurs de stocker des données de santé d'individus de manière sécurisée tout en proposant aux personnes concernées de mettre ces données à la disposition de chercheurs contre rémunération. Healthbank a laissé entendre qu'elle pourrait adopter la technologie *blockchain* dans un futur proche.

Le format de la présente contribution ne permet pas de procéder à un examen détaillé des différents modèles proposés. Un tel exercice est d'ailleurs particulièrement délicat en raison de leur caractère évolutif et de leur haute technicité. Ceux-ci présentent toutefois souvent des caractéristiques générales communes qu'il est possible de synthétiser de la manière suivante.

En raison de limitations techniques, l'entreposage du contenu intégral d'un dossier médical sur une *blockchain* n'est pas envisageable[32]. Le volume des données médicales est en effet trop important pour les capacités de la technologie *blockchain*. La grande majorité des modèles se limitent donc à l'enregistrement de métadonnées[33]. Ces métadonnées se rapportent généralement au détenteur des données de santé, à la localisation des données et aux autorisations d'accès[34]. Immuables et accessibles depuis n'importe où, elles font en principe l'objet d'un cryptage qui permet de confirmer l'existence des données ainsi que leur intégrité sans dévoiler leur contenu[35].

26 DAGHER *et al.*
27 Voir : <www.cccinnovationcenter.com>.
28 Par exemple : YUE *et al.*
29 Le lecteur intéressé par un aperçu plus large des projets menés dans le domaine pourra par exemple consulter les sites web relatifs aux projets ou entreprises suivants : « *Guardtime* », « *Gem Health Network* », « *Medicalchain* », « *Medibloc* », « *Medicohealth* », « *Medilot* » ou encore « *BurstIQ* ».
30 Voir : <www.myhealthmydata.eu>. Parmi les acteurs engagés dans la recherche figure notamment la HES-SO.
31 DUBOVITSKAYA *et al.,* p. 654 ss.
32 LINN/KOO, p. 4.
33 Une métadonnée est une donnée qui sert à définir, caractériser ou décrire une autre donnée.
34 Par exemple MedRec : AZARIA *et al*., p. 26.
35 BAXENDALE, p. 39.

L'entreposage primaire des dossiers médicaux continuerait d'être assumé de manière décentralisée par les fournisseurs de soins (les métadonnées renvoient à la localisation des données)[36]. Certains auteurs prônent toutefois la centralisation informatique des dossiers médicaux dans un lieu d'entreposage unique, parfois désigné « *data lake* »[37]. Cela étant, que l'entreposage informatique des dossiers médicaux continue à relever de la responsabilité des fournisseurs de soins ou qu'il soit centralisé auprès d'un hébergeur unique, la technologie *blockchain* ne semble pas en mesure d'assurer une sécurité plus efficace des données de santé. Dans la mesure où ces dernières sont entreposées en dehors de la *blockchain* (« *off-chain* »), elles restent en grande partie exposées aux risques classiques de piratage, à plus forte raison lorsqu'elles sont centralisées puisqu'elles offrent alors un point unique de défaillance[38].

Élément central des modèles proposés, le recours aux « contrats intelligents » permet au patient de contrôler les accès à son dossier médical. Selon les modèles, il peut choisir d'octroyer des autorisations d'accès au dossier et déterminer quelles informations peuvent être communiquées, éventuellement dans quelle limite de temps. Les « contrats intelligents » permettraient au surplus d'intégrer les hypothèses dans lesquelles la loi autorise l'accès au dossier médical par des tiers[39]. Sur la *blockchain*, l'identité du patient n'est pas anonymisée, mais pseudonymisée selon des méthodes qui diffèrent selon les modèles. En principe, même si l'identité du patient reste privée, la consultation de l'historique de la *blockchain* permettrait par exemple de constater qu'un même individu a consulté un même fournisseur de soins à plusieurs reprises sur une période donnée[40]. De telles informations couplées à des informations externes pourraient, selon les situations, permettre la réidentification du patient[41].

En raison du caractère particulièrement sensible des données de santé, la grande majorité des modèles recourent à des *blockchains* privées avec des acteurs autorisés et des accès contrôlés. Les risques de réidentification, mêmes faibles, excluent le recours aux *blockchains* publiques avec ou sans permission[42]. Une autre question – épineuse – consiste à déterminer qui gère et entretient les différents nœuds informatiques de la *blockchain* privée. Ce travail est coûteux et énergivore. Selon les modèles, il pourrait s'agir des institutions de soins d'un même réseau, mais aussi d'acteurs publics ou d'institutions de recherche[43].

Le recours à la technologie *blockchain* devrait permettre de mieux harmoniser les intérêts *a priori* divergents que sont la protection des données de santé et l'accès aux données de santé par des tiers[44]. Les modèles proposés visent en effet à renforcer les droits des patients en améliorant leur contrôle sur les données de santé. L'intégrité et l'exhaustivité du dossier médical seraient mieux assurées grâce à l'horodatage systématique des opérations qui y seraient effectuées. En tant qu'effet indirect, le recours à la *blockchain* impliquerait de surcroît une meilleure uniformisation des données et

36 AZARIA *et al.,* p. 26 ; LINN/KOO, p. 4.
37 LINN/KOO, p. 4.
38 DÉZIEL, p. 91.
39 Par exemple : LINN/KOO, p. 4.
40 AZARIA *et al*., p. 30.
41 *Ibid*.
42 Par exemple : MCFARLANE *et al.,* p. 6 ; LINN/KOO, p. 3.
43 Par exemple : AZARIA *et al.,* p. 29.
44 DÉZIEL, p. 86 ss ; AZARIA *et al.,* p. 26.

contribuerait à amenuiser les difficultés d'interopérabilité des données de santé. La technologie *blockchain* aurait ainsi le potentiel de réduire les problèmes causés par le nombre important d'intermédiaires qui détiennent des données[45]. Dans le même temps, l'adoption d'un cadre avec un point d'entrée unique favoriserait les accès – contrôlés et autorisés – aux données de santé par des tiers, que ce soit par exemple à des fins curatives (ex. : réseaux des soins), de recherche ou de surveillance épidémiologique. Elle contribuerait ainsi à mieux harmoniser le système de soins, à prévenir certaines atteintes et à réduire les coûts de la santé[46].

2. Protection des données de santé et secret médical

Bien qu'elles se trouvent encore à un stade de développement précoce, les applications *blockchain* pour la gestion des dossiers médicaux laissent entrevoir des perspectives prometteuses. Elles soulèvent toutefois un certain nombre de questions juridiques, dont les principales ont été sélectionnées pour être traitées dans le présent chapitre.

a) Réglementation hétérogène et complexe des données de santé

En Suisse, la gestion des dossiers médicaux par les soignants ou les établissements de soins relève essentiellement du droit de la protection des données, du champ de protection renforcé du secret médical (lorsqu'il est applicable) et du droit cantonal sanitaire. En raison du fédéralisme et de l'adoption progressive de nouvelles normes au cours des dernières décennies, la protection des données de santé est aujourd'hui soumise à un régime réglementaire particulièrement hétérogène et complexe[47]. Le contenu des dossiers médicaux et leurs conditions de conservation – en particulier la durée de conservation – relèvent principalement du droit cantonal sanitaire[48]. L'obligation faite aux soignants d'observer le secret médical relève quant à elle principalement du droit fédéral (art. 321 CP[49], art. 320 CP, art. 35 LPD[50]), mais peut aussi dépendre – alternativement ou cumulativement – du droit cantonal sanitaire, du droit cantonal de la protection des données ou de lois spéciales selon le champ d'application personnel de chacune de ces lois. Notons au passage que les législations fédérale et cantonales de protection des données désignent les données en lien avec la santé comme des données « *sensibles* » et leur confèrent une protection renforcée. La multiplicité des lois applicables se révèle particulièrement épineuse lorsqu'il s'agit de déterminer les cas où des données de santé peuvent ou doivent être communiquées à des tiers. En principe, la règle de base de toute communication d'informations couvertes par le secret médical est le consentement du patient (notamment art. 321 ch. 2 CP). Des dispositions légales fédérales ou cantonales peuvent

45 KUO/KIM/OHNO-MACHADO, p. 1214.
46 MCFARLANE *et al*., p. 2.
47 Pour un aperçu général des différentes normes applicables au secret médical et aux difficultés posées par leur coordination, voir par exemple : BURGAT, p. 225.
48 26 cantons et autant de lois sanitaires.
49 RS 311.0.
50 RS 235.1.

toutefois statuer des obligations ou des autorisations d'informer une autorité ou de témoigner en justice (notamment art. 321 ch. 3 CP). Aujourd'hui, ces exceptions légales au secret médical – énoncées de manière plus ou moins précise – sont disséminées dans une multitude de textes de rang fédéral et cantonal. Les soignants soumis au secret médical peuvent demander à l'autorité cantonale compétente de les délier du secret en dehors des cas prévus par la loi (art. 321 ch. 2 CP, mais aussi droit cantonal sanitaire). De nouvelles difficultés surgissent ensuite quant au sort des données après leur communication à des tiers. À cet égard, la gestion des données de santé par les assurances sociales et privées, soumises à des règles différenciées, illustre de manière particulièrement marquante les écueils réglementaires en la matière. À titre d'exemple, l'article 33 de la loi fédérale sur la partie générale du droit des assurances sociales (LPGA)[51] impose une obligation générale de garder le secret à toutes les personnes qui participent à l'application des lois sur les assurances sociales. Ce principe de base est toutefois largement atténué par les dispositions des législations spéciales en matière d'assurances sociales qui autorisent, sous forme de listes particulièrement larges et complexes, la communication de données traitées à d'autres tiers à toute sorte de fins[52].

Ce bref panorama – non exhaustif – suffit à mettre en exergue une problématique importante : la conservation des données de santé et leur communication à des tiers ne dépendent pas uniquement de la volonté du patient, mais d'une réglementation complexe et disparate, parfois imprévisible (ex. : levée du secret par l'autorité). Or, les modèles *blockchain* de gestion des dossiers médicaux reposent essentiellement sur le consentement du patient et tendent à délaisser les communications à des tiers autorisées ou imposées par la loi. Dans certains modèles, il est simplement prévu de « programmer » les communications imposées dans la loi au moyen de contrats intelligents. Au regard de la complexité et de l'imprévisibilité de la réglementation suisse, la programmation de ces communications constitue un défi important. L'intention de redonner le pouvoir au patient est certes louable, mais il faut garder à l'esprit que le bon fonctionnement d'un système de santé repose sur une gestion fluide et réactive des données de santé tout en leur assurant une protection forte.

b) Champ d'application des réglementations applicables

Comme expliqué, les modèles *blockchain* de gestion des données de santé excluent le stockage des informations médicales directement sur la *blockchain*, notamment pour des questions techniques. Les données enregistrées se limitent à des métadonnées cryptées qui renvoient généralement au détenteur des données de santé, à la localisation des données et aux autorisations d'accès. Il faut également ajouter aux métadonnées les adresses individuelles des différents acteurs (patients, soignants, etc.) qui permettent de retracer leurs activités sur la *blockchain*. Le stockage « *off chain* » des dossiers médicaux sert parfois d'argument à ceux qui entendent exclure les *blockchains* du champ d'application des réglementations de protection des données de santé.

Renoncer à une *blockchain* publique pour recourir à une *blockchain* privée ou publique avec autorisation pour la gestion des dossiers médicaux n'exclut pas l'application des législations fédérale ou cantonales sur la protection des données. La loi fédérale sur la protection des données

51 RS 830.1.

52 Voir par exemple : art. 84a LAMal, RS 832.10 ; art. 97 LAA, RS 832.20.

régit par exemple le traitement de données concernant des personnes physiques ou morales effectué par des personnes privées ou des organes fédéraux[53]. Elle exclut certes de son champ d'application les données personnelles qu'une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers[54]. Toutefois, les *blockchains* impliquent par principe un partage d'informations entre les différents nœuds informatiques qui les composent, même dans les *blockchains* privées. Les personnes physiques (ex. : un médecin privé) qui recourraient à une *blockchain* privée ne pourraient donc pas se prévaloir de cette exception. Il en va de même pour le champ d'application des lois cantonales sur la protection des données qui règlent les traitements de données effectués par des organes publics cantonaux. Dès lors que ces derniers traitent des données personnelles – et à plus forte raison des données de santé sensibles –, ils sont soumis aux réglementations cantonales sur la protection des données[55]. Quant aux règles imposant un devoir de confidentialité aux soignants (ex. : art. 321 CP, art. 320 CP), elles ne sont en rien influencées par le choix d'une *blockchain* publique ou privée. Le soignant qui recueille les informations couvertes par le secret médical peut uniquement les communiquer à des tiers s'il y est autorisé par le patient, par la loi ou par l'autorité. Que ces révélations injustifiées interviennent dans un cadre public ou privé n'a pas d'importance.

Plus discutable est la question de savoir si les données traitées sur la *blockchain* sont des données « *personnelles* ». La LPD définit les données personnelles comme toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 3 let. a LPD). Ainsi, seules les données strictement anonymes sortent du champ d'application des législations de protection des données et des principes qui les régissent. La notion de « *personne identifiable* » n'est pas forcément facile à appréhender. Selon le Conseil fédéral, « *est réputée identifiable la personne physique qui peut être identifiée, directement ou indirectement, c'est-à-dire par corrélation d'informations tirées des circonstances ou du contexte.* »[56] Le Conseil fédéral précise cependant que « *si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre (…), on ne peut guère parler de possibilité d'identification. Il convient de prendre en compte dans chaque cas d'espèce l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne.* »[57] Dans l'arrêt *Logistep* du 8 septembre 2010, le Tribunal fédéral a cependant interprété la notion de personne identifiable de manière large en admettant que les adresses IP dynamiques constituaient des données personnelles au sens de l'article 3 let. a LPD[58].

Sur la *blockchain*, les adresses individuelles des différents acteurs ainsi que les métadonnées enregistrées ne sont pas anonymisées au sens strict, mais seulement pseudonymisées au moyen de techniques cryptographiques[59]. Pour certains auteurs, cela suffit à maintenir le caractère personnel

53 Art. 2 al. 1 LPD.
54 Art. 2 al. 2 let. LPD.
55 À mon sens, le recours à une *blockchain* par des organes publics devrait d'ailleurs être expressément prévu par une loi en vertu de l'article 5 Cst.
56 Message du Conseil fédéral du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (ci-après : « Message révision totale LPD »), FF 2017 6565, 6639. Sur cette question, voir aussi : ISLER, p. 9.
57 Message révision totale LPD, FF 2017 6565, p. 6639-6640.
58 ATF 136 II 508, c. 3, JdT 2011 II 446.
59 STENGEL/AUS DER AU, p. 445.

des données, d'autant plus que l'effort à fournir pour rattacher une personne physique à une adresse n'est pas forcément considérable[60]. C'est en particulier le cas lorsqu'il est possible de procéder à des recoupements avec des informations extérieures, par exemple lorsque la consultation de la *blockchain* permet de déterminer qu'un même individu a fréquenté régulièrement un même établissement sanitaire dans une période donnée[61]. Bien que l'analyse dépende toujours des circonstances particulières, il n'apparaît pas déraisonnable de partir du principe que les données traitées sur une *blockchain* en lien avec la gestion des dossiers médicaux constituent des données personnelles.

Un raisonnement similaire peut être appliqué à l'obligation d'observer le secret médical (art. 321 CP, art. 320 CP, droit cantonal sanitaire), qui ne s'applique pas aux communications de données anonymes. En raison des risques de réidentification, le soignant qui enregistre des informations en lien avec un patient sur une *blockchain* doit le faire dans le respect des règles relatives au secret médical.

c) Consentement du patient

Les modèles *blockchain* de gestion des dossiers médicaux cherchent en premier lieu à renforcer le consentement du patient face aux demandes d'accès à son dossier médical par des tiers. D'un point de vue juridique, les modèles proposés impliquent toutefois deux consentements distincts :

- le consentement du patient à ce que des tiers puissent accéder aux informations contenues dans le dossier médical. Ce consentement est programmé sur la *blockchain* par le patient au moyen d'un contrat intelligent ;

- le consentement préalable du patient à ce que des informations le concernant (métadonnées) soient enregistrées sur la *blockchain*, en particulier par l'action du soignant.

Alors que les développeurs des différents modèles se concentrent systématiquement sur le premier consentement, le second consentement est habituellement laissé de côté. Il est pourtant fondamental puisqu'il délie le soignant du secret médical (art. 321 ch. 2 CP notamment) et l'autorise à enregistrer des informations couvertes par le secret médical sur la *blockchain*. Ce consentement est soumis à un certain nombre de conditions. Il ne doit pas être excessif au sens de l'article 27 al. 2 CC[62] et doit pouvoir être révoqué en tout temps[63]. La validité du consentement d'un patient à l'inscription permanente de métadonnées relatives à sa santé paraît non seulement questionnable au regard des engagements excessifs, mais aussi du point de vue de l'effectivité d'une éventuelle révocation. Sous l'angle du secret médical, l'exigence du consentement pourrait être contournée par l'adoption d'une base légale (art. 321 ch. 2 CP), mais l'admissibilité d'une telle base légale est questionnable.

60 *Ibid.* ; ISLER, p. 10 ; BERBERICH/STEINER, p. 423-424.
61 Problématique notamment soulignée par DUBOVITSKAYA *et al.*, p. 650 ; MCFARLANE *et al.*; p. 6 et DAGHER *et al.,* p. 296.
62 RS 210.
63 ERARD/GUILLOD, p. 9.

d) Permanence des données enregistrées

Même si les dossiers médicaux sont entreposés « *off chain* », les informations inscrites sur la *blockchain* (métadonnées, traces d'accès, etc.) sont inaltérables et ne peuvent donc pas être effacées. Dans le domaine sensible de la santé, le patient peut souhaiter l'effacement de ses données pour de multiples raisons : maladies stigmatisantes, traitement considéré comme injustifié par le patient, prévention des risques liés aux nouvelles technologies (piratage) ou simplement garder une mainmise sur ses données personnelles.

Sur la base des articles 13 al. 2 Cst. (protection de la sphère privée), 10. al. 2 Cst. (droit à la liberté personnelle) et 8 § 1 CEDH (droit au respect de la vie privée et familiale), le Tribunal fédéral a reconnu l'existence d'un droit fondamental à l'« *autodétermination informationnelle* »[64]. Celui-ci confère un droit de maîtrise sur ses données personnelles, en particulier le droit de déterminer soi-même si et dans quels buts ces données peuvent être traitées. Toute une série de droits sont déduits du droit fondamental à l'autodétermination informationnelle, dont celui de s'opposer à un traitement de données ou le droit à la rectification des données[65]. Si elle est opérée par une entité étatique, la conservation en tout ou partie du dossier médical contre la volonté du patient constitue une atteinte à son droit fondamental à l'autodétermination informationnelle. Elle doit donc être justifiée aux conditions habituelles de restriction des droits fondamentaux, à savoir reposer sur une base légale, être justifiée par un intérêt public et respecter le principe de proportionnalité (art. 36 Cst.). Si l'une de ces conditions fait défaut, le traitement de données est illicite et doit cesser. En d'autres termes, le patient peut requérir la destruction des données concernées[66].

En ce qui concerne le respect des droits fondamentaux entre personnes privées, l'article 35 al. 3 Cst. énonce que « *les autorités veillent à ce que les droits fondamentaux, dans la mesure où ils s'y prêtent, soient aussi réalisés dans les relations qui lient les particuliers entre eux.* » En matière de protection des données de santé, la mise en œuvre du droit à l'autodétermination informationnelle est principalement assurée par les dispositions de la loi fédérale sur la protection des données et par les législations cantonales sanitaires qui imposent des devoirs aux soignants indépendamment de leur statut privé ou public. Aux termes de l'article 4 al. 1 et 2 LPD, tout traitement de données doit être licite et respecter le principe de la proportionnalité.

Que ce soit dans le cadre d'un traitement de données par une entité publique ou par une personne privée, le concept de proportionnalité est central dans la discussion de la destruction de données. Il prohibe en particulier la conservation de données personnelles au-delà de ce qui est nécessaire pour atteindre les buts prévus lors de la collecte et s'oppose ainsi aux « *fichages* » sans limite de temps[67]. C'est principalement sur cette base que repose le « *droit à l'oubli* ».

Quelques législations cantonales sanitaires prévoient expressément la destruction du dossier médical. À Genève, le dossier médical doit par exemple être détruit après vingt ans au plus tard si

64 ATF 138 II 346, c. 8.2, JdT 2013 I 71.
65 ERARD/AMEY, p. 277 et réf. citées.
66 *Idem*, p. 290.
67 WALTER, p. 2.

aucun intérêt prépondérant pour la santé du patient ou pour la santé publique ne s'y oppose et si la réglementation sur les archives publiques ne prévoit pas un délai plus long[68].

À première vue, un modèle *blockchain* de gestion des dossiers médicaux implique l'enregistrement irréversible de données concernant le traitement d'un patient. Même s'il s'agit d'une partie minime du dossier médical, ces informations restent particulièrement sensibles. L'impossibilité d'effacer ces données sur le long terme, même justifiée par une base légale, semble donc poser des difficultés de compatibilité avec le principe de proportionnalité imposé par le droit suisse.

Même s'il paraît plus anecdotique ici en raison de la nature des données enregistrées sur la *blockchain*, le droit du patient à la rectification des données traitées (ex. : art. 5 al. 2 LPD) paraît lui aussi mis à mal. La technologie *blockchain* permet certes d'enregistrer de nouvelles données, corrigées, mais elle ne permet pas d'effacer les données inexactes.

3. Loi fédérale sur le dossier électronique du patient

En plus des obstacles déjà mentionnés, la conception d'un système *blockchain* de gestion des dossiers médicaux en Suisse devrait impérativement assurer un niveau d'harmonisation suffisant avec le dossier électronique du patient (« DEP »). La mise en œuvre du DEP est régie par la loi fédérale sur le dossier électronique du patient (« LDEP »)[69] et ses différentes ordonnances. L'adoption des structures nécessaires pour le lancement du DEP est en cours et ce dernier devrait être opérationnel dans toute la Suisse au plus tard en 2020.

Dans les grandes lignes, le DEP est défini par la loi comme un « *dossier virtuel permettant de rendre accessibles en ligne, en cas de traitement concret, des données pertinentes pour ce traitement qui sont tirées du dossier médical d'un patient et enregistrées de manière décentralisée ou des données saisies par le patient lui-même* »[70]. La mise en œuvre fait coexister deux types de systèmes informatiques : les systèmes primaires et les systèmes secondaires. Les systèmes primaires sont les systèmes informatiques traditionnels d'entreposage des dossiers médicaux (informatisés) des patients. Le DEP est un système secondaire, distinct des systèmes primaires, qui contient uniquement les données tirées du dossier médical pertinentes pour un traitement concret[71]. En principe, le soignant décide quelles données présentent une pertinence suffisante pour être insérées dans le DEP, mais le patient peut lui-même y insérer des données. Dans tous les cas, le DEP ne se confond pas avec le dossier médical principal et ne peut le remplacer.

La structure générale du DEP est décentralisée : les professionnels de la santé, les institutions et les patients sont affiliés à des communautés régionales dont la tâche consiste principalement à assurer la disponibilité des données enregistrées dans les DEP. Le professionnel de la santé qui souhaite consulter des informations relatives à un patient dans un autre établissement de soins doit déposer une requête en ligne auprès de la communauté à laquelle il est affilié. La communauté questionne

68 Art. 57 Loi sur la santé, RS-GE K 1 03.
69 RS 816.1.
70 Art. 2 let. a LDEP.
71 Art. 2 let. a LDEP.

ensuite l'ensemble des autres communautés pour établir la liste de tous les documents mis à disposition du DEP pour le patient concerné. Si le patient l'a autorisé, le professionnel de la santé pourra alors consulter à distance les informations mises à disposition par d'autres professionnels de la santé dans le DEP. Chaque traitement de données doit être consigné dans un historique[72]. Le droit d'accès est librement modulable par le patient, qui peut attribuer différents niveaux de confidentialité aux données du DEP, autoriser l'accès à des groupes de professionnels ou encore limiter les autorisations dans le temps[73].

L'affiliation au DEP est facultative pour le patient[74]. Les professionnels de la santé sont également libres de proposer ou non le DEP, à l'exception notable des fournisseurs de prestations au sens des articles 39 et 49a LAMal (établissements stationnaires tels que les hôpitaux, les maisons de naissance et les EMS) qui sont obligés de proposer le DEP à leurs patients. Le caractère facultatif du DEP ne permet pas pour l'heure de garantir son adoption massive dans le futur.

En l'état actuel de la réglementation, les données mises à disposition du DEP sont uniquement exploitables en vue du traitement des patients. Selon le Conseil fédéral, la LDEP n'a pas été conçue pour le développement de registres de maladies ou de qualité, à des fins de statistiques ou de recherche en vue d'optimiser des processus administratifs. De telles utilisations ne sont pas exclues, mais devraient être prévues par des législations spéciales[75].

Il est intéressant de noter que la LDEP poursuit des buts similaires à ceux prônés par les concepteurs de modèles de gestion des dossiers médicaux basés sur la technologie *blockchain*, en particulier l'augmentation de la sécurité des patients, une meilleure efficacité du système de santé et le développement des compétences des patients en matière de santé[76]. Dans les modèles *blockchain*, le recours à la technologie vise toutefois à conférer au patient un contrôle plus fort sur ses données personnelles. Ces modèles visent de surcroît à contrôler l'accès au dossier médical primaire – en d'autres termes à l'information originale – et non secondaire, comme cela est prévu pour le DEP. La multiplication des autorités pourrait également être désignée comme un point faible du DEP face à la *blockchain*, puisque le patient doit se fier non seulement à l'institution qui détient son dossier médical, mais aussi aux communautés et à leurs sous-traitants chargés d'entreposer les données qui le concernent. Pour autant, le DEP n'est pas exempt d'avantages. Il paraît plus souple, favorise les échanges fluides et permet la prise en compte de situations particulières, notamment d'urgence.

Le DEP et des modèles *blockchains* visent à fournir des services semblables et fonctionnent selon une logique de base pour le moins similaire. Ainsi, à première vue, l'implantation d'un système *blockchain* en marge du DEP – par exemple à l'échelle régionale ou d'un réseau d'établissements de soins – semble difficile à mettre en œuvre. Elle impliquerait un dédoublement kafkaïen de toute une série de mécanismes (autorisations du patient, double niveau de métadonnées, etc.).

72 Art. 10 al. 1 let. LDEP.
73 Art. 1 al. 1 et 2, art. 4 Ordonnance sur le dossier électronique du patient (ODEP), RS 816.11.
74 Art. 3 al. 1 LDEP.
75 Message du Conseil fédéral du 29 mai 2013 concernant la loi fédérale sur le dossier électronique du patient (LDEIP), FF 2013 4747, p. 4796.
76 Art. 1 al. 3 LDEP.

D'un point de vue pratique, la seule application envisageable de la technologie *blockchain* pour la gestion des dossiers médicaux passe certainement par une intégration directement dans le DEP. Ce dernier fonctionne en effet déjà sur la base de registres de métadonnées (au niveau des communautés) qui pourraient éventuellement être conciliés avec la technologie *blockchain*. Comme ces registres couvrent uniquement le référencement d'une partie des données du patient (données importantes pour le traitement), le recours à la technologie *blockchain* pourrait cependant perdre en attractivité.

IV. Autres applications dans le domaine de la santé

Des propositions ont été émises pour recourir à la technologie *blockchain* dans d'autres secteurs en lien avec la santé. La présente section se limite à un bref aperçu de quelques-unes d'entre elles. Dès le moment où des données personnelles sont traitées sur la *blockchain*, les considérations du chapitre précédent peuvent servir de base de réflexion, sans toutefois remplacer une analyse juridique circonstanciée.

La technologie *blockchain* pourrait servir d'outil pour mieux encadrer la recherche biomédicale, notamment grâce aux possibilités d'authentification, de traçabilité et d'horodatage des données[77]. Les protocoles de recherche, les consentements des sujets de recherche ou encore les plans d'analyse statistique pourraient être enregistrés sur une *blockchain* de telle manière que les résultats puissent être contrôlés. Les sujets de recherche pourraient suivre l'évolution des étapes de la recherche, consentir ou non à l'utilisation de leurs données en cas de modification du protocole de recherche et accepter de partager leurs données pour d'autres recherches. Par ailleurs, le recours aux « contrats intelligents » pourrait permettre de lier les étapes d'une même recherche en conditionnant le commencement d'une nouvelle étape à l'introduction sur la *blockchain* des résultats obtenus à l'étape précédente[78].

La *blockchain* semble également offrir des perspectives particulièrement attrayantes pour la lutte contre les contrefaçons de médicaments[79]. Du point de vue de la traçabilité, cette technologie permettrait de tenir un registre public, transnational et infalsifiable de toutes les étapes de mise sur le marché, de la production en usine jusqu'à la remise au comptoir, sans reposer sur une autorité centrale[80]. Un tel renforcement de la traçabilité s'inscrirait dans la droite ligne des obligations imposées par la Convention du Conseil de l'Europe sur la contrefaçon de produits médicaux et les infractions similaires menaçant la santé publique (« Convention MEDICRIME ») qui est entrée en vigueur pour la Suisse le 1er janvier 2019. Par rapport aux dossiers médicaux, la traçabilité des

77 BENCHOUFI/RAVAUD, p. 2 ss ; ROMAN-BELMONTE/DE LA CORTE-RODRIGUEZ/RODRIGUEZ-MERCHAN, p. 422 ; DUBOVITSKAYA *et al.,* p. 653

78 BENCHOUFI/RAVAUD, p. 2 ss.

79 METTLER, p. 2.

80 Voir par exemple : TSENG *et al.* ; MACKEY/NAYYAR, p. 596.

produits thérapeutiques n'implique en principe pas le traitement de données personnelles et échappe donc aux écueils posés par les législations de protection des données.

D'autres projets proposent par exemple de recourir à la technologie *blockchain* pour rendre les systèmes d'assurance plus rapides et efficaces[81], y compris à l'échelle internationale, ou encore pour renforcer le cadre d'exercice des professions médicales (ex. : certification des diplômes)[82].

Conclusion

La technologie *blockchain* apporte des pistes de réflexion intéressantes pour la gestion des dossiers médicaux. À première vue, elle renforcerait les droits des patients sur leurs données dans un contexte où le besoin d'accès aux données de santé par des tiers se fait toujours plus pressant. Elle permettrait en même temps à ces tiers d'accéder à de plus larges volumes de données de santé lorsqu'ils y sont autorisés.

L'introduction en Suisse d'un système de gestion des dossiers médicaux basés sur la technologie *blockchain* se confronte cependant à plusieurs obstacles juridiques. L'enregistrement de données personnelles sur une *blockchain* – même sous forme de métadonnées – suscite toute une série d'interrogations du point de vue de l'obligation des soignants d'observer le secret médical, de la prise en compte des régimes hétérogènes imposés par les législations fédérales et cantonales sur la conservation et la gestion des données de santé, du consentement du patient à ce que ses données soient traitées sur une *blockchain* ou encore de l'impossibilité d'effacer les données. En raison du caractère encore émergent de la technologie, on ne peut pas conclure *a priori* que ces obstacles sont rédhibitoires. Les concepteurs de ces modèles devront cependant proposer des solutions compatibles avec ces exigences sous peine d'inapplicabilité juridique. D'un point de vue structurel, l'introduction d'un système *blockchain* de gestion des dossiers médicaux en Suisse devrait s'intégrer harmonieusement au DEP. À cet égard, seule une intégration de la technologie *blockchain* au sein même du DEP semble envisageable. Une intégration en marge du DEP deviendrait vite impraticable en raison du dédoublement des structures.

Plus généralement, on peut se demander si les bénéfices apportés par la technologie *blockchain* sont suffisamment importants pour justifier son intégration dans les systèmes de gestion des dossiers médicaux en dépit de toutes les incertitudes juridiques et pratiques suscitées. Renforcer le pouvoir

[81] IVAN, p. 8, propose un exemple d'application en matière d'assurance où les assureurs dûment certifiés pourraient, par recours à un contrat intelligent lié au dossier médical, questionner ce dernier pour obtenir la preuve que des soins ont été fournis conformément aux conditions posées pour le remboursement. Par exemple, dans le cas d'un patient diagnostiqué avec un diabète de type 2, l'assureur pourrait questionner le dossier médical pour déterminer si le patient a subi un dépistage rétinien au cours de l'année précédente. La mise en œuvre du contrat intelligent se contenterait d'apporter la réponse : oui, non ou sans objet. Le calcul des prestations pourrait ainsi être effectué en limitant de manière importante la communication de données personnelles.

[82] ROMAN-BELMONTE/DE LA CORTE-RODRIGUEZ/RODRIGUEZ-MERCHAN, p. 421 ss. Pour différentes applications dans le domaine de la santé, voir également : GORDON/WRIGHT/LANDMAN.

du patient en lui offrant un consentement fort est un objectif louable, mais un système de santé fonctionnel doit pouvoir compter sur des échanges d'informations fluides. Ces interrogations sont d'autant plus pertinentes que les modèles proposés reposent sur des *blockchains* privées, gérées par un cercle d'acteurs fermé. On reste donc assez éloigné de la suppression totale des intermédiaires promise par les *blockchains* publiques. En conclusion, la *blockchain* a certainement un avenir dans le domaine de la santé, mais celui-ci se limitera peut-être en priorité aux secteurs exempts de données personnelles tels que celui de la traçabilité des produits thérapeutiques.

Bibliographie

ANGRAAL Suveen/KRUMHOLZ Harlan M./SCHULTZ Wade L., « Blockchain Technology. Applications in Health Care », in Circulation : Cardiovascular Quality and Outcomes 2017/9, en ligne : <www.ahajournals.org/doi/10.1161/ CIRCOUTCOMES.117.003800> (cité : ANGRAAL/KRUMHOLZ/SCHULZ).

AZARIA Asaph *et al.,* « MedRec : Using Blockchain for Medical Data and Permission Management », in 2016 IEEE 2nd International Conference on Open and BigData du 22 au 24 août 2016 à Vienne, p. 25 ss, en ligne : <https://ieeexplore-ieee-org.proxy3.library.mcgill.ca/document/7573685> (cité : AZARIA *et al.*).

BAXENDALE Gareth, « Can Blockchain Revolutionise EPRs ? », in ITNOW 2016/1, p. 38 ss (cité : BAXENDALE).

BENCHOUFI Mehdi/RAVAUD Philippe, « Blockchain technology for improving clinical research quality », in Trials 2017, en ligne : <https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z> (cité : BENCHOUFI/RAVAUD).

BERBERICH Matthias/STEINER Malgorzata, « Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers ? », in European Data Protection Law Review 2016/3, p. 422 ss (cité : BERBERICH/STEINER).

BURGAT Sabrina, « Le secret médical – Interférences et interdépendances entre droit privé et droit public », in DUNAND Jean-Philippe/MAHON Pascal (édit.), *« Le droit décloisonné », interférences et interdépendances entre droit privé et droit public*, Genève 2009, p. 225 ss (cité : BURGAT).

DAGHER Gaby G. *et al*., « Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology », in Sustainable Cities and Society 2018/39, p. 283 ss (cité : DAGHER *et al*.).

DÉZIEL Pierre-Luc, « La frontière technologique : les *blockchains*, le partage de renseignements personnels sur la santé et le droit à la vie privée au Canada », in RÉGIS Catherine/KHOURY Lara/KOURI Robert P. (édit.), *Health Law at the Frontier / Les rencontres en droit de la santé – Volume 2*, Montréal 2018, p. 67 ss (cité : DÉZIEL).

DUBOVITSKAYA Alevtina *et al.,* « Secure and Trustable Electronic Medical Records Sharing using Blockchain », in AMIA Annual Symposium Proceedings Archive 2017, p. 650 ss (cité : DUBOVITSKAYA *et al*.).

ERARD Frédéric/AMEY Laura, « La destruction du dossier médical sur requête du patient sous l'angle du droit public », in DUPONT Anne-Sylvie/GUILLOD Olivier (édit.), Réflexions romandes en droit de la santé, Bâle 2016, p. 277 ss (cité : ERARD/AMEY).

ERARD Frédéric/GUILLOD Olivier, « Levée générale du secret médical et assistance au suicide », in : Jusletter 29 janvier 2018 (cité : ERARD/GUILLOD).

GORDON William/WRIGHT Adam/LANDMAN Adam, « Blockchain in Health Care : Decoding the Hype », in The New England Journal of Medicine Catalyst 2017, en ligne : <https://catalyst.nejm.org/decoding-blockchain-technology-health> (cité : GORDON/WRIGHT/LANDMAN).

ISLER Michael, « Datenschutz auf der Blockchain », in Jusletter 4 décembre 2017 (cité : ISLER).

IVAN Drew, « Moving Toward a Blockchain-based Method for the Secure Storage of patient Records », soumission primée dans le cadre du concours « Blockchain and Its Emerging Role in Healthcare and Health-related Research » initié par le Office of the national Coordinator for Health Information Technology américain, 2016, en ligne : <www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf> (cité : IVAN).

KUO Tsung-Ting/KIM Hyeon-Eui/OHNO-MACHADO Lucila, « Blockchain distributed ledger technologies for biomedical and health care applications », in Journal of the American Medical Informatics Association 2017/6, p. 1211 ss (cité : KUO/KIM/OHNO-MACHADO).

LINN Laure/KOO Martha, « Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research », soumission primée dans le cadre du concours « Blockchain and Its Emerging Role in Healthcare and Health-related Research » initié par le Office of the national Coordinator for Health Information Technology américain, 2016, en ligne : <www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf> (cité : LINN/KOO).

MACKEY Tim K./NAYYAR Gaurvika, « A review of existing and emerging digital technologies to combat the global trade in fake medicines », in Expert Opinion on Drug Safety 2017/5, p. 587 ss (cité : MACKEY/NAYYAR).

MCFARLANE Chrissa ET AL., « Patientory : A Healthcare Peer-to-Peer EMR Storage Network v1.1 », 2017, en ligne : <https://patientory.com/patientory_white paper.pdf> (cité : MCFARLANE *et al.*).

METTLER Matthias, « Blockchain Technology in Healthcare. The Revolution Starts Here », in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) du 14 au 17 septembre 2016 à Munich, en ligne : <https://ieeexplore.ieee.org/document/7749510> (cité : METTLER).

OULD YAHIA Youcef/PARADINAS Pierre, « Applications e-santé, le contrôle des données personnelles. Un enjeu majeur pour la protection de la vie privée », in La Protection des

données face à la menace cyber, C&ESAR du 27 au 29 novembre 2017 à Rennes, en ligne : <www.cesar-conference.org/wp-content/uploads/2017/11/Actes_Cesar_2017_Protection_donn%C3%A9es_et_menace_cyber_v2.pdf> (cité : OULD YAHIA/PARADINAS).

PETERSON Kevin *et al.,* « A blockchain-Based Approach to Health Information Exchange Networks », soumission primée dans le cadre du concours « Blockchain and Its Emerging Role in Healthcare and Health-related Research » initié par le Office of the national Coordinator for Health Information Technology américain, 2016, en ligne : <www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf> (cité : PETERSON *et al*.).

RIEDER Philip/LOUIS-COURVOISIER Micheline/HUBER Philippe, « The end of medical confidentiality? Patients, physicians and the state in history », in Medical Humanities 2016/3, p. 149 ss (cité : RIEDER/LOUIS-COURVOISIER/HUBER).

ROMAN-BELMONTE Juan M./DE LA CORTE-RODRIGUEZ Hortensia/RODRIGUEZ-MERCHAN E. Carlos, « How blockchain technology can change medicin », in Postgraduate Medicine 2018/4, p. 420 ss (cité : ROMAN-BELMONTE/DE LA CORTE-RODRIGUEZ/RODRIGUEZ-MERCHAN).

STENGEL Cornelia/AUS DER AU Roman, « Blockchain : Eine Technologie für effektiven Datenschutz ? », in sic! 2018/9, p. 439 ss (cité : STENGEL/AUS DER AU).

TSENG Jen-Hung *et al*., « Governance on the Drug Supply Chain via Gcoin Blockchain », in Environmental Research and Public Health 2018/6, en ligne : <www.ncbi.nlm.nih.gov/pmc/articles/PMC6025275> (cité : TSENG *et al.*).

WALTER Jean-Philippe, « Le droit à l'oubli : la perspective européenne », in : CEDIDAC, Le droit à l'oubli : du mythe à la réalité, Colloque du 20 novembre 2014 à Lausanne, en ligne : <www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/le-pfpdt-dans-les-medias.html> (cité : WALTER).

WRIGHT Aaron/DE FILIPPI Primavera, « Decentralized Blockchain Technology and the Rise of *Lex Crypotgraphia* », 2015, en ligne : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> (cité : WRIGHT/DE FILIPPI).

YUE Xiao *et al*., « Healthcare Data Gateways : Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control », in Journal of Medical Systems 2016/10, p. 217 (cité : YUE *et al.*).