cognitio

studentisches Forum für Recht und Gesellschaft

Le conservatisme de la protection des données face à la révolution blockchain

LUBOMIR CANTER

Zitiervorschlag

CANTER, Le conservatisme de la protection des données face à la révolution blockchain, in: cognitio 2019/1.

URL: cognitio-zeitschrift.ch/2019-1/Canter

DOI: https://doi.org/10.5281/zenodo.2836661

ISSN: 2624-8417

cognitio

studentisches Forum für Recht und Gesellschaft

Le conservatisme de la protection des données face à la révolution blockchain

LUBOMIR CANTER, MLaw Unifr/Master de droit comparé Paris II Panthéon-Assas, Intern at CA Indosuez (Switzerland) SA in the Legal & Structuring Desk[1]

Blockchain ist eine revolutionäre Technologie mit einem umfangreichen Anwendungsgebiet. Umso mehr stellt Blockchain aufgrund der Struktur der Technologie eine grosse Herausforderung für den Datenschutz dar. Werden diese Inkompatibilitäten einen Einfluss auf die Entwicklung der Blockchain haben? Oder wird Blockchain den regulatorischen Rahmenbedingungen des Datenschutzes entgehen?

La blockchain est une révolution et possède de domaines d'application multiples. Néanmoins la blockchain pose de grands défis à la protection des données du fait de sa structure même. Ces incompatibilités nuiront-elles au développement de la blockchain? Ou la blockchain échappe-t-elle au champ réglementaire de la protection des données?

Blockchain is a revolution and has an extensive field of application. Nevertheless, blockchain is a big challenge for data protection due to the structure of this technology. Will these incompatibilities affect blockchain development? Or will blockchain escape the regulatory framework of data protection?

Sommaire

[1] L'auteur remercie sincèrement le Professeur Dr. Marc Amstutz, LL.M. (Harv.), Freiburg i.Üe et Jan Hendrik Ritter, MLaw pour leur aide respective dans la rédaction et la publication de ce travail.

I. Introduction

L'essor technologique et numérique de ces dernières années a permis beaucoup d'avancés, non sans poser de nombreuses questions en matière de protection de la vie privée de l'utilisateur. De nombreux acteurs du monde technologique sont fréquemment accusés de ne pas suffisamment se soucier du respect des données personnelles des utilisateurs.[2] Parmi les nouvelles technologies, la blockchain s'est emparée de l'actualité en 2017. Depuis cette date, il ne passe pas un jour où une publication ne lui soit pas consacrée ou qu'un nouveau domaine d'application ne lui soit attribuée. Cette technologie, issue des cryptomonnaies, est promise à un avenir prometteur. Sa relation avec le droit est ambiguë, tant elle tend à s'affranchir des règles juridiques classiques.[3] Une réflexion est ainsi menée par certains,[4] afin de déterminer si le droit positif peut intégrer une technologie aussi disruptive que la blockchain ou si, au contraire, le droit doit s'adapter et se réformer pour pouvoir intégrer cette nouvelle technologie. Cette question est particulièrement dynamique dans la relation que la blockchain entretient avec la protection des données.[5] Cette dernière constitue également un des sujets majeurs de notre époque. Le législateur suisse a entrepris une révision de la LPD (Loi fédérale sur la protection des données, RS 235.1). L'Union européenne (UE) a quant à elle introduit le RGPD (Règlement du Parlement européen et du Conseil 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), applicable depuis le 25 mai 2018. Si le droit cherche à protéger les données des citoyens, il est possible de se poser la question de savoir si la technologie, et notamment la technologie blockchain, ne pourrait-elle pas participer à la protection de ses utilisateurs, peut-être même, de manière plus efficace que les règles de droit prévues à cet effet. A l'inverse, il est possible de se demander également si la protection accordée aux données personnelles elle ne constitue pas un frein au développement technologique en général et de la blockchain en particulier. Le fondateur de la monnaie Ethereum ainsi que de sa blockchain Vitalik Buterin, voit dans la protection des données un des enjeux majeurs de la blockchain.[6] Tout au long de cet article, nous allons voir que si la blockchain peut contribuer à une protection efficace des données, sa structure et son fonctionnement

2 Voir le scandale Facebook-Cambridge Analytica: ROSENBERG MATTHEW/CONFESSORE NICHOLAS/CADWALLADR CAROLE, How Trump Consultants Exploited the Facebook Data of Millions, The New York Times, 17 mars 2018; tous les sites web visités le 15 mai 2019.

3 SIMMONS & SIMMONS LLP, Le droit et la technologie blockchain: Une approche sectorielle, Contrats, Concurrence, Consommation, 10/2017, nº 1.

4 SIMMONS & SIMMONS LLP (Fn. 3), nº 1.

5 DEROULEZ JÉRÔME, Blockchain et données personnelles – Quelle protection de la vie privée? La semaine juridique, Edition générale, 38/2017, nº 4.

6 BUTERIN VITALIK, Privacy on the Blockchain, 2016, in: Privacy on the Blockchain, p. 1.

vont à l'encontre des principes de la protection des données.

II. La Blockchain: outil révolutionnaire utile à la protection des données

La blockchain s'est développée grâce aux cryptomonnaies. Cette technologie trouve des applications dans une multitude de domaines, notamment dans la protection des données.

A. Origine et fonctionnement de la blockchain

1. La blockchain au service des cryptomonnaies

La blockchain peut se définir comme «une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle».[7] Support aux transactions effectuées par les cryptomonnaies,[8] la blockchain permet de réaliser une transaction mais aussi de s'assurer que cette dernière a véritablement été réalisée.[9] Cette technologie est ainsi un élément essentiel au fonctionnement des cryptomonnaies. Le mystérieux créateur du Bitcoin, Satoshi Nakamoto,[10] l'a en effet utilisé comme outil de stockage permettant d'effectuer les transactions de la première des cryptomonnaies.

La blockchain fonctionne grâce à un livre comptable recensant l'ensemble des transactions effectuées[11] mentionnant également l'heure, la date, le montant et les signatures cryptées de ces transactions codées.[12] Si le Bitcoin a pendant longtemps été beaucoup plus médiatisé que la technologie blockchain permettant de le mettre en œuvre, cette dernière est désormais beaucoup étudiée tant ses applications sont variées[13] (santé, assurance, authentification de documents, contrats, droits d'auteur, sécurisation du vote, moyen de paiement, streaming en ligne, etc.).

2. Une technologie révolutionnaire dans son fonctionnement

La blockchain dispose de plusieurs atouts majeurs. Elle est sécurisée, inviolable, non falsifiable et n'est pas contrôlée par une autorité ou une personne[14] mais par l'ensemble de sa communauté ce qui offre une garantie d'indépendance. La blockchain ne nécessite pas dans son fonctionnement du tiers de confiance[15] que peut constituer la banque. La confiance des contreparties ne réside pas en la banque, acteur neutre, mais dans le code. Pour les utilisateurs de la blockchain: code is law.

---

7 Blockchain France, Découvrir la blockchain.

8 DEROULEZ (Fn. 5), nº 7; GRÜNEWALD SERAINA, Währungs- und Geldwäschereirechtliche Fragen bei virtuellen Währungen, in: Weber Rolf/Thouvenin Florent (édit.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zurich 2015, p. 103.

9 POPPE MORGANE/VERBIEST THIBAULT, Quelle relation entre la protection des données à caractère personnel et la blockchain, Revue Lamy Droit des Affaires, 129/2017, p. 38.

10 GRAHAM-SIEGENTHALER BARABARA/FURRER ANDREAS, The Position of Blockchain Technology and Bitcoin in Swiss Law, Jusletter, 8 mai 2018, nº 1; MARTIN-FORISSIER CAROLINE, Blockchain et RGPD, une union impossible?, Laboratoire d'Innovation Numérique de la CNIL, 24 août 2017.

11 BRENDER NATHALIE/GAUTHIER MARION, Impacts de la blockchain sur le métier d'auditeur, EF 6–7/2018, p. 444; MÉTILLE SYLVAIN, Internet et droit – Protection de la personnalité et questions pratiques, Zurich 2017, p. 23; DE PREUX PASCAL/TRAJILOVIC DANIEL, Blockchain et lutte contre le blanchiment d'argent – Le nouveau paradoxe? EF 1-2/2018, p. 61; SIMMONS & SIMMONS LLP (Fn. 3), nº 2.

12 BRENDER/GAUTHIER (Fn. 11), p. 444.

13 EVERDELL CHRISTIAN/MANDELL DANIEL, White-Collar Crime, The promise of Blockchain Technology To Combat Money Laundering, The New York Law Journal, 62/2017, p. 9.

14 BRENDER/GAUTHIER (Fn. 11), p. 444 et 445 ; CHAFIOL FLORENCE/BARBET-MASSIN ALICE, La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données, Dalloz, Droit de la propriété intellectuelle et du numérique, 12/2017, p. 637; DEROULEZ (Fn. 5), nº 3; GRYNBAUM LUC, Assurance et Blockchain, Revue Lamy Droit des Affaires, 129/2017, p. 53.

15 MARTIN-FORISSIER (Fn. 10); SIMMONS & SIMMONS LLP (Fn. 3), nº 2.

L'outil blockchain est décentralisé car la solution ne se trouve pas sur un ordinateur, mais sur une multitude d'ordinateurs décentralisés qui constituent des nœuds de réseau,[16] reliés en réseau pair à pair (peer to peer networks).[17] Les nœuds valident des clefs cryptographiques[18] et contribuent ainsi au fonctionnement de la blockchain en délivrant des solutions permettant des usages différents, comme celui de réaliser une transaction en cryptomonnaies ou de valider un smart contract.

Les mineurs sont les individus qui font vivre la blockchain. Ils jouent un rôle crucial dans le fonctionnement de la blockchain car ce sont eux qui sont derrières les nœuds de réseau et qui valident les transactions en résolvant des problèmes. Ils doivent, afin de toucher une rémunération, envoyer une preuve de travail (proof of work).[19] Les mineurs sont rémunérés pour leur travail en cryptomonnaies. En effet, le travail de mineur nécessite un important investissement en matériel informatique et est extrêmement couteux en énergie.[20] Ce coût environnemental pourrait d'ailleurs potentiellement entraver, tout comme la protection des données (cf. infra III), l'économie des cryptomonnaies mais aussi la blockchain.

Plusieurs types de blockchain existent. La blockchain à caractère public, utilisée pour le Bitcoin, l'Ethereum[21] ou le Dash, est par essence ouverte à toute personne souhaitant y participer.[22] Aucun tiers de confiance ne s'assure du bon fonctionnement de la blockchain publique. Les mineurs y participent de manière égalitaire et les décisions y sont validées à la majorité des utilisateurs.[23] Ouverte à tous, les données qui y sont contenues sont également accessibles à l'ensemble des participants. Ce type de blockchain, utilisée par le Bitcoin, ne repose pas sur la confiance accordée aux mineurs, mais en leur nombre grâce au protocole de consensus (consensus protocol).[24] Une majorité de mineurs doivent valider les nœuds validant ainsi l'opération.[25]

A l'inverse, la blockchain privée, n'est ouverte qu'aux utilisateurs acceptés et identifiés disposants d'autorisations[26] délivrées par un gérant.[27] C'est le cas de la cryptomonnaie Ripple utilisée par des établissements financiers.[28] Certains d'entre eux (Crédit Agricole notamment) développent une blockchain privée à l'usage du secteur des matières premières: Komgo.[29] Pour un auteur, la blockchain privée «ne s'agirait pas d'une véritable blockchain».[30] Si nous ne souscrivons pas totalement à ce postulat, force est de constater que ce type de blockchain va à l'encontre de la philosophie initiale de la blockchain en instaurant une autorité à la tête de la blockchain. Ainsi, l'utilisateur désirant s'assurer que la validation d'opérations soit restreinte à un groupe limité de personnes de confiance serait inspiré d'avoir recours à la blockchain privée. En effet, le caractère infalsifiable de la blockchain ne garantit pas

16 CHAFIOL/BARBET-MASSIN (Fn. 14), p. 637; MARTIN-FORISSIER (Fn. 10); DE PREUX/TRAJILOVIC (Fn. 11), p. 61.

17 GRAHAM-SIEGENTHALER/FURRER (Fn. 10), nº 2.

18 DEROULEZ (Fn. 5), nº 7 ; DE PREUX/TRAJILOVIC (Fn. 11), p. 61.

19 FARINE MATHILDE, Le bitcoin, désastre écologique en perspective?, Le Temps, 12 novembre 2017.

20 FARINE (Fn. 19).

21 MEYER DAVID, Blockchain technology is on a collision course with EU privacy law, The International Association of Privacy Professionals, 27 février 2018.

22 CANIVET GUY, Blockchain et régulation, Semaine juridique entreprises et affaires, 36/2017, p. 39.

23 CHAFIOL/BARBET-MASSIN (Fn. 14), p. 638; LE TROCQUER ANNE-HÉLÉNE, Blockchain, gouvernance d'entreprise et infrastructures de marchés, Revue Lamy Droit des Affaires, 129/2017, p. 45.

24 BERKE ALLISON, How safe are blockchains? It depends, Harvard Business Review, 7 Mars 2017.

25 BERKE (Fn. 24).

26 LE TROCQUER (Fn. 23), p. 45.

27 CANIVET (Fn. 22), p. 39; CHAFIOL/BARBET-MASSIN (Fn. 14), p. 638.

28 MEYER (Fn. 21).

29 CERTES NICOLAS, 15 sociétés, dont BNP Paribas et Crédit Agricole, créent la plateforme blockchain Komgo, Le Monde Informatique, 20 septembre 2018.

30 CANIVET (Fn. 22), p. 39.

pour autant l'exactitude des informations validées.

Enfin, à mi-chemin entre les deux précédentes, la blockchain hybride, également appelée consortium[31] est en partie décentralisée. Elle est contrôlée par des parties authentifiées laissant l'accès à l'utilisateur ou en interdisant ou limitant son accès.[32]

B. La protection des données

1. La protection des données en Suisse

La LPD régit en Suisse la protection des données. Avant son introduction en 1991, les dispositions générales de l'art. 28 ss CC (Code civil suisse du 10 décembre 1907, RS 210) sur la protection de la sphère privée régissaient les données personnelles.[33] Néanmoins, avec l'essor de l'informatique, d'internet et de la récolte de données, la protection offerte par l'art. 28 CC s'est révélée insuffisante. La LPD en tant que loi atechnologique[34] s'adapte plus facilement aux évolutions en matière de données personnelles et des technologies permettant d'y recourir. Cette loi a notamment su anticiper les bouleversements du big data et a été longtemps considérée comme un texte de loi allant plus loin que d'autres législations étrangères.[35] En effet, des simples données servant à effectuer un profil de la personnalité plus ou moins précis constituent des données formant le profil de la personnalité. C'est précisément ce que fait le big data, en récoltant différentes données sur des personnes, et qui une fois réunies ensemble, permettent de dresser le profil d'une personne. Cependant, cette loi résonne comme peu protectrice à l'égard des personnes par rapport à la récente réglementation européenne.

2. La protection des données en UE

Le droit européen s'est également impliqué dans la protection des données. C'est d'abord, la directive 95/46/CE posait déjà les jalons de la protection des données en Europe. Un projet de révision a été entrepris à partir de 2012, conduisant à l'entrée en vigueur du RGPD le 25 mai 2018. Ce dernier étend son emprise en dehors des frontières de l'UE. En effet, une entreprise située en dehors de l'UE mais proposant des services à des citoyens européens ou sur le marché européen se voit appliquer ce règlement. De ce fait de nombreuses entreprises suisses doivent désormais prendre en compte cette nouvelle réglementation (art. 3 RGPD).[36]

Avec le RGPD, la protection des données ne peut plus être considérée pour les entreprises ou les organisations comme secondaire. Le RGPD introduit en effet de nombreuses nouveautés dans les règles sur la protection des données: la création d'un poste de délégué à la protection des données (art. 37 RGPD), l'obligation de se préoccuper de la protection des données lors de la conception du projet (privacy by design, art. 25 al. 1 RGPD) et de n'utiliser que les données nécessaires au regard de la finalité du traitement (privacy by default, art. 25 al. 2 RGPD),[37] le droit à l'effacement des données (art. 17 RGPD) ainsi que l'obligation de communiquer à l'autorité nationale la violation de données à caractère personnel (art. 33 RGPD). Des sanctions sont également prévues à l'encontre des entreprises ne mettant pas en place les obligations imposées par le RGPD. Ces sanctions peuvent atteindre 4 % du chiffre d'affaires mondial ou jusqu'à 20 millions d'euros d'amende.[38]

---

31 MEKKI MUSTAPHA, Les Mystères de la blockchain, Recueil Dalloz, 37/2017, p. 2160 ss, nº 5.

32 LE TROCQUER (Fn. 23), p. 45; MEKKI (Fn. 31), nº 5.

33 MEIER PHILIPPE/DE LUZE ESTELLE, Droit des personnes, art. 11–89a CC, Genève, Zurich, Bâle 2014, nº 922.

34 CHABOT FLAVIO-GABRIEL, La protection des données à la lumière de deux exemples tirés de l'actualité récente, Centre du droit de l'entreprise de l'Université de Lausanne, 57/2011, p. 1.

35 MEIER/DE LUZE (Fn. 33), nº 928 et 930.

36 CERESOLA SERGIO, Actualités sur le droit de la protection des données: nouveautés dans l'UE et en Suisse, Expert Focus 3/2018, p. 179; PRAZ EMILIE, Responsabilités et outils de conformité selon la RGPD, Pratique juridique actuelle, 5/2018, p. 609.

37 PRAZ (Fn. 36), p. 612.

38 CERESOLA (Fn. 36), p. 179. L'entreprise américaine Google a d'ailleurs écopé d'une sanction de 50 millions d'euros prononcé par l'autorité

Si la Suisse a pendant longtemps, par l'intermédiaire de la LPD, eu une législation efficace pour protéger les données, le RGPD va beaucoup plus loin que la LPD. Conscient de l'importance du RGPD, le législateur suisse a entrepris une révision totale de la LPD afin de la rapprocher des dispositions du droit européen,[39] sans pour autant les unifier.

C. La blockchain comme outil de sécurisation des données

1. Avantages et applications de la blockchain dans la protection des données

La blockchain fut, comme nous avons pu le voir, développée dans le cadre des cryptomonnaies pour effectuer des transactions sécurisées. Elle permet d'assurer une grande confidentialité à ses utilisateurs.[40]

Parmi les multiples utilisations pouvant être faite de cette technologie, la blockchain constitue un formidable outil de récolte et de stockage de données.[41] Elle peut dès lors être utilisée afin de contenir des données personnelles.[42] Cette technologie révolutionnaire permet en effet de sécuriser toutes sortes de données sur un réseau décentralisé que tout utilisateur peut librement consulter dans un grand livre comptable.[43] Une fois que ces données sont stockées, elles ne peuvent plus être modifiées.[44] Un tel procédé sécurisé permet de faire confiance aux informations retranscrites sur la blockchain. La protection des données et la blockchain peuvent avoir un fonctionnement similaire en ayant tous deux recours à la cryptographie pour garantir l'anonymat des utilisateurs.[45] Pour être réellement efficace, la blockchain doit être animée par un nombre important de mineurs afin d'être rendue fiable.[46] Mais de manière paradoxale, cette sécurité est aussi une faiblesse de la blockchain par rapport à la protection des données (cf. infra III.C.5).

Les médecins pourraient ainsi se servir de la blockchain pour stocker le consentement de leurs patients. Dans ce cas, le formulaire de consentement du patient serait intégré sous forme codée à la blockchain, garantissant l'anonymat du patient, où il serait conservé.[47]

La blockchain pourrait s'avérer également utile dans les fonctions de compliance au sein des banques,[48] où elle permettrait de vérifier plus rapidement la validité des identités des parties à la transaction.[49]

Les mots de passe pour accéder aux réseaux sociaux sont peu fiables car facilement piratables. L'ambitieux Onename vise à remplacer les mots de passe que l'internaute utilise pour se connecter sur les réseaux sociaux ou sur les sites des administrations publiques. L'objectif étant de simplifier les nombreux mots de passe qu'un internaute peut avoir à gérer, mais aussi de le protéger contre les

française veillant notamment au respect de la protection des données: la CNIL (Commission nationale de l'informatique et des libertés): La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société Google LLC, 21 janvier 2019.

39 Message 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, FF 2017 I 1084, p. 6567.

40 DEROULEZ (Fn. 5), nº 15.

41 DEROULEZ (Fn. 5), nº 8; MOUGAYAR WILLIAM, Business Blockchain – Pratiques et applications professionnelles, Paris 2017, p. 46 et 47; POPPE/VERBIEST (Fn. 9), p. 38.

42 POPPE/VERBIEST (Fn. 9), p. 38.

43 DEROULEZ (Fn. 5), nº 8; EVERDELL/MANDELL (Fn. 13), p. 9; GRAHAM-SIEGENTHALER/FURRER (Fn. 10), nº 120; DE PREUX/TRAJILOVIC (Fn. 11), p. 61.

44 DE PREUX/TRAJILOVIC (Fn. 11), p. 61.

45 DEROULEZ (Fn. 5), nº 5.

46 NAFTALSKI FABRICE/REVOL SOPHIE/FAUVEL LOUISE, Blockchain et protection des données personnelles, EY Société d'avocat, 12 juillet 2018.

47 THÉARD-JALLU CÉCILE, La blockchain au service de la santé? L'exemple de la collecte du consentement du patient dans un essai clinique, Revue Lamy Droit des Affaires, 129/2017, p. 42.

48 EVERDELL/MANDELL (Fn. 13), p. 9; DE PREUX/TRAJILOVIC (Fn. 11), p. 61.

49 DEROULEZ (Fn. 5), nº 13.

risques d'usurpations par des tiers.[50] Grâce à ce système, l'utilisateur va s'y enregistrer sans avoir à inscrire son adresse, sa date de naissance, ou son sexe.[51] Pour s'identifier sur un site tel que Facebook, il devra prouver qu'il est bien le détenteur du compte auquel il souhaite accéder en publiant un contenu permettant à d'autres utilisateurs de vérifier, grâce à la blockchain, qu'il s'agit bien de lui. Ce modèle peine cependant à se développer et à devenir l'outil incontournable d'identification en ligne basé sur la blockchain.

La reconnaissance vocale et faciale permet de protéger les utilisateurs contre des usurpations d'identité sur les réseaux sociaux ou de s'identifier face à des banques ou des administrations. Les sociétés Accenture et Microsoft travaillent sur le système de reconnaissance faciale ID 2020. Ce dernier projet basé sur la blockchain permet de créer une identité digitale sécurisée offrant un accès aux services internet à des personnes ne pouvant prouver leur identité faute de documents, comme par exemple les réfugiés de guerres ou climatiques.[52] Ce système porterait selon ses développeurs, un très haut niveau de sécurité et de protection des données.[53]

TITANIUM (Tools for the Investigation of Transactions in Underground Markets) vise à lutter contre l'utilisation de la blockchain à des fins criminelles.[54] Mis en place par 15 États européens, ce projet se donne pour ambition de développer la lutte contre la criminalité informatique de manière compatible avec la protection des données des utilisateurs de cette technologie.[55]

2. La Suisse: lieu propice au développement de la blockchain et des cryptomonnaies

Dans la lutte que de nombreux pays se livrent pour devenir le centre mondial des cryptomonnaies et de la blockchain, la Suisse se place comme un acteur incontournable dans ces domaines. L'EPFL a récemment mis en place un système permettant de procéder à des votes en ligne au moyen de la blockchain. Selon l'École fédérale de Lausanne, le procédé est totalement sécurisé contre les risques d'attaques informatiques, notamment les bourrages d'urnes virtuels et garantit une protection des données efficace.[56]

Le canton de Zoug, surnommé la «Crypto-Valley», apparaît comme un précurseur dans l'usage des cryptomonnaies, grâce à ses nombreuses start-ups actives dans le secteur. Zurich n'est pas en reste, où il est possible de retirer de l'argent liquide contre des cryptomonnaies.[57] En Suisse romande, Genève espère devenir la capitale des cryptomonnaies et de la blockchain. Les autorités suisses ont compris le rôle que sont amenées à jouer les cryptomonnaies: l'autorité financière suisse, la FINMA, a diffusé des guidelines en matière d'ICO (Initial Coin Offering) afin d'encadrer juridiquement cette nouvelle technique de financement, équivalente d'une IPO (Initial Public Offering) dans le domaine des cryptomonnaies.[58]

Le succès de la Suisse dans ce domaine s'explique grâce à une loi sur la protection des données efficiente mais surtout peu contraignante. La grande stabilité politique du

50 REYNAUD FLORIAN, Onename, un curieux projet de carte d'identité numérique, Le Monde, 3 février 2016.

51 Ibidem.

52 Accenture, Microsoft create blockchain solution to support ID 2020, Accenture, 19 juin 2017 (cité: ACCENTURE).

53 ACCENTURE (Fn. 52).

54 Project to prevent criminal use of the dark web and virtual currencies launched by international consortium, Tools for the Investigation of Transactions in Underground Markets, 19 mai 2017 (cité: TITANIUM).

55 TITANIUM (Fn. 54).

56 AUBORT SARAH, La blockchain au secours du vote électronique: une première à l'EPFL, EPFL, 29 juin 2018.

57 AWP, La Suisse à la pointe des cryptomonnaies, Bilan, 29 mars 2018.

58 FINMA, Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO), 16 février 2018.

pays[59] et des infrastructures informatiques de qualité, expliquent cette appétence pour la blockchain et plus largement pour l'innovation.[60] De plus, le degré de formation élevé ainsi que l'ouverture sur le monde et aux affaires participent également à l'attractivité du pays dans le domaine des cryptomonnaies et de la blockchain en Suisse.

III. Une technologie difficilement compatible avec la protection des données

Si la blockchain peut être utile à la protection des données, cette dernière régule aussi la blockchain. Or, il apparaît que la blockchain de par son fonctionnement et son utilisation
ne respecte pas la protection des données en général et le RGPD en particulier. Des solutions sont possibles, mais elles vont à l'encontre de la philosophie libertaire de la blockchain.

A. Une technologie soumise à la protection des données

La blockchain est considérée par beaucoup comme un processus parfaitement anonyme ne permettant pas de remonter aux personnes y ayant recours. Néanmoins, une identification de l'utilisateur semble possible.[61] En effet, le gouvernement britannique dans un rapport avait montré que l'anonymat n'était pas totalement garanti, car les transactions du fait de leur caractère public pouvaient être tracées.[62]

De surcroit, la blockchain contient des données personnelles dès lors que les informations s'y trouvant se rapportent à une personne identifiée ou pouvant l'être grâce à la clef cryptographique.[63] Or, la blockchain, en tant qu'instrument servant par essence à stocker des données, a de nombreuses chances de contenir des données personnelles l'assujettissant dès lors aux règlementations sur la protection des données. Aussi, la blockchain contient toujours des données se rapportant indirectement à son utilisateur: la clé publique avec laquelle celui-ci effectue l'opération.[64] Cette clé publique, constitue une donnée personnelle en application du considérant l'art. 26 RGPD édictant qu'une personne physique est identifiable dès qu'elle peut être reconnue de manière directe ou indirecte. Dans ce cas, la protection des données s'applique à la personne. Le droit européen,[65] tout comme le droit suisse,[66] avait déjà considéré que constituait une donnée personnelle l'adresse IP (Internet Protocol)[67] d'un ordinateur, même lorsque celle-ci est dynamique (l'adresse IP change à chaque connexion).[68]

L'anonymat de l'utilisateur, nous l'avons vu, n'est pas absolu dans la blockchain. L'information que cette dernière contient (adresse postale, numéro de compte, montant de la transaction, etc.) l'est encore moins. Au contraire, il s'agit d'ailleurs de la philosophie première de la blockchain, à savoir effectuer une opération qui peut être connue de tous.[69] Or, lorsque des données concernant des personnes physiques déterminées ou identifiables sont échangées sur la blockchain, il s'agit d'un traitement de données,

59 Interview de Guido RUDOLPHI, La «blockchain», une technologie numérique capable de changer le monde?, RTS, 2 mai 2016.

60 EMBASSY OF THE KINGDOM OF THE NETHERLANDS IN BERN, Blockchain in Switzerland – Opportunities for future cooperation between Switzerland and the Netherlands, Berne 2018, p. 18.

61 NAFTALSKI/REVOL/FAUVEL (Fn. 46) ; POPPE/VERBIEST (Fn. 9), p. 39.

62 WALPORT MARK, Distributed ledger technology beyond blockchain, UK Government Office for Science, p. 50–51.

63 SIMMONS & SIMMONS LLP (Fn. 3), nº 9.

64 SIDE AUDREY/MOLLET-VIEVILLE BENJAMIN/CORDIN AUGUSTIN, La blockchain et la protection des données personnelles, mémoire, Paris-Est Créteil 2018.

65 CJUE, Arrêt Patrick Beyer c/Bundesrepublik Deutschland C-582/14, EU:C:2016:779.

66 ATF 136 II 508, consid. 3, JdT 2011 II 446.

67 POPPE/VERBIEST (Fn. 9), p. 39.

68 POPPE/VERBIEST (Fn. 9), p. 39.

69 SIDE/MOLLET-VIEVILLE/CORDIN (Fn. 64), p. 14.

encadré par le nouveau RGPD.[70] Blockchain Partner, société active dans le conseil sur la blockchain, considère en revanche que la blockchain peut être amenée à contenir des données personnelles sans pour autant se voir appliquer le RGPD. Car la blockchain ne dispose pas de responsable du traitement défini à l'art. 4 al. 7 RGPD.[71] Nous sommes en désaccord avec cette argumentation affranchissant du droit une technologie au motif que la régulation juridique ne saurait s'appliquer du fait de l'absence d'un caractère essentiel. Dans ces situations où la règle de droit ne peut s'appliquer directement du fait de l'absence d'un caractère essentiel, le droit ne disparaît pas. Au contraire, le droit y remédie en créant la fonction. Néanmoins, ce point de vue visant à considérer que la blockchain ne peut pas être assujettie à la règle de droit, car trop disruptive et que le droit n'est pas adapté à une telle technologie illustre la relation conflictuelle ente la règle de droit et la blockchain.

Il convient de souligner que le type de traitement varie selon que la blockchain soit de nature publique ou privée.[72] La blockchain publique, du fait de l'absence d'autorité de contrôle, mais aussi du caractère public des informations y étant contenue, est problématique dans sa relation avec la protection des données. Elle ne protège pas les données personnelles qui sont accessibles à toute personne consultant le grand livre comptable. Son caractère bien que semi-public pour certains,[73] ne constitue pas une garantie efficiente de protection des données. A l'inverse, les obstacles à la protection des données inhérents à la blockchain, peuvent être résolus dans la blockchain privée. La solution passe par une contractualisation des relations entre les participants désignant un responsable du traitement des données ainsi que les droits et obligations des parties en matière de protection des données.[74]

B. Un fonctionnement et une utilisation opaques à l'opposé de la protection des données

La blockchain dans son état actuel suscite encore beaucoup la méfiance des citoyens.[75] La blockchain présente, c'est certain, des caractéristiques difficilement compatibles avec la protection des données.[76] C'est la blockchain publique, ouverte à tous, qui pose le plus de problème par rapport à sa compatibilité avec la protection des données. La réglementer paraît difficile[77] du fait de sa structure sans aucune autorité de contrôle pouvant mettre en application les exigences réglementaires. Autorité de contrôle, allant justement à l'encontre de la philosophie libertaire de la blockchain.

L'outil de sécurisation des données que peut constituer la blockchain peut aussi être utilisé afin de masquer l'identité des parties. C'est d'ailleurs l'un des buts de cette technologie.[78] Cette protection de l'anonymat, nécessaire et compréhensible dans certaines situations, peut aussi être utilisé à des fins néfastes. La blockchain et par voie de conséquence les cryptomonnaies, par leur fonctionnement, permettent à des criminels de masquer l'origine litigieuse des fonds[79] et permettent de blanchir l'argent sale, opérer des transactions douteuses et financer le trafic de drogue ou le terrorisme.[80]

S'il s'agit d'un sujet différent de celui de la protection des données, il ne lui est pas totalement étranger. La protection des données

70 SIMMONS & SIMMONS LLP (Fn. 3), p. 5.

71 O'RORKE WILLIAM, Blockchain et GDPR: le grand malentendu, Blockchain Partner, 23 novembre 2017.

72 CHAFIOL/BARBET-MASSIN (Fn. 14), p. 637 ss.

73 MOUGAYAR (Fn. 41), p. 46.

74 POPPE/VERBIEST (Fn. 9), p. 38.

75 ODOXA, Blockchain: un a priori négatif des français qui la connaissent encore très mal, 10 mai 2018. Ce sondage montre que 68 % des français estiment que la blockchain est une technologie détruisant des emplois.

76 DEROULEZ (Fn. 5), nº 9.

77 LE TROCQUER (Fn. 23), p. 45; POPPE/VERBIEST (Fn. 9), p. 38.

78 UK GOVERNMENT OFFICE FOR SCIENCE (Fn. 62), p. 50.

79 EVERDELL/MANDELL (Fn. 13), p. 9; DE PREUX/TRAJILOVIC (Fn. 11), p. 61.

80 DEROULEZ (Fn. 5), nº 5.

ne garantit pas l'anonymat sans limites, notamment lorsque d'autres exigences légales doivent également être appliquées comme c'est le cas de la lutte contre le blanchiment d'argent.[81] Or, la blockchain, dans une transaction Bitcoin par exemple, n'enregistrera que peu de données (adresses Bitcoin des parties, le montant, la date et l'heure du transfert). Cette forme d'anonymat rend difficile, mais non impossible comme nous avons pu le voir, un traçage de l'expéditeur et du bénéficiaire des fonds.[82] C'est à ce titre l'utilisation qui était faite du Bitcoin sur Silk road, un site du darkweb qui permettait de se faire livrer chez soi un large choix de produits prohibés.[83]

La blockchain et ses applications peuvent être utilisées à des fins néfastes allant à l'encontre des règles de compliance. Elle peut aussi lui être utile. Il eut en effet été possible d'imaginer un système de blockchain privée tenu par les banques contenant l'ensemble du KYC (know your customer) de leurs clients et permettant une lutte efficace contre le blanchiment d'argent par un large partage d'informations.[84] Pareil projet visant à ce que les banques s'échangent des données sur des clients se heurte au secret bancaire et à la protection des données et ne peut ainsi être mis en place.

La blockchain est un outil révolutionnaire au très fort potentiel pouvant avoir un impact extrêmement bénéfique sur l'économie. Cependant, il est largement incompatible avec la protection des données. La blockchain et ses soutiens doivent, s'ils veulent respecter la protection des données, consentir à d'importants changements dans l'essence même de la blockchain, risquant néanmoins de la dénaturer. Car en dehors de la pression réglementaire, des concurrents à cette technologie existent: confidentialité différentielle, systèmes partiellement homomorphes ou encore calcul sécurisé.[85]

C. Une incompatibilité surmontable avec le RGPD

1. L'absence d'un responsable du traitement dans la blockchain publique

Le RGPD instaure en son art. 24 al. 1 une nouvelle fonction au sein des entreprises procédant à des traitements de données. Le Compliance Officer s'occupe au sein d'une banque de s'assurer de la conformité du fonctionnement de la banque à la réglementation nationale et internationale. Le Data Protection Officer doit dorénavant s'assurer du respect de la réglementation en matière de protection des données pour le compte du responsable du traitement.[86]

Or, la blockchain publique, en tant qu'instrument décentralisé, rend difficile voire impossible[87] l'identification d'un responsable et dès lors de son éventuel sous-traitant. Au contraire, dans la blockchain privée, il suffit d'en nommer un.[88] Ainsi, en cas de violation des données personnelles ou de simple demande d'une personne dans une blockchain publique, les obligations imposées par le RGPD ne peuvent être remplies.[89] Au contraire d'une blockchain privée, qui est gérée par une autorité pouvant mettre en place les exigences imposées par le RGPD.

Pour remédier à cette incompatibilité majeure entre la blockchain publique et le

81 DEROULEZ (Fn. 5), nº 11. Sur la relation entre-nue entre le secret bancaire et la protection des données voir: JACOT-GUILLARMOD EMILIE/HIRSCH CÉLIAN, Le secret bancaire est mort vive la protection des données!, Le Temps, 10 décembre 2018.

82 EVERDELL/MANDELL (Fn. 13), p. 9. Bien que nous ayons vu que les transactions effectuées au moyen de la blockchain ne permettent pas un anonymat total.

83 EVERDELL/MANDELL (Fn. 13), p. 9. Sur Silk road: voir le documentaire Deep Web.

84 DE PREUX/TRAJILOVIC (Fn. 11), p. 70.

85 DEROULEZ (Fn. 5), nº 14.

86 PRAZ EMILIE M., Responsabilités et outils de conformité selon la RGPD, PJA 2018, p. 609.

87 LEGEAIS DOMINIQUE, Blockchain et données personnelles: réponse de la CNIL, JCP Entreprises et Affaires, 41/2018, p. 9; POPPE/VERBIEST (Fn. 9), p. 39.

88 NAFTALSKI/REVOL/FAUVEL (Fn. 46).

89 POPPE/VERBIEST (Fn. 9), p. 39.

RGPD, certains auteurs proposent de considérer comme responsable la personne à l'origine de l'application ou du smart contract lorsque celle-ci est identifiable.[90]
L'autorité de surveillance française des protections
des données, la CNIL, considère que les responsables du traitement pourraient être les utilisateurs de la blockchain lorsqu'ils y soumettent une opération aux mineurs.[91]
Si au contraire, il est considéré que ce n'est pas aux acteurs de la blockchain d'être considérés comme les responsables du traitement, il serait aussi possible d'attribuer ce rôle aux sites hébergeant la blockchain.[92]

2. Le rôle du mineur dans la protection des données

Si les solutions vues précédemment (supra III.C.1) permettent difficilement d'identifier un responsable dans la blockchain publique, une alternative pourrait exister.

Le mineur de la blockchain, pourrait lui-même être considéré selon certains comme le
responsable de la blockchain.[93] Néanmoins, nous considérons que le mineur ne saurait être considéré comme responsable dans la mesure où il se cantonne à exécuter des opérations ordonnées par les utilisateurs.

L'art. 28 RGPD permet au responsable du traitement de déléguer le traitement à un sous-traitant. Ce dernier doit selon les exigences du même article présenter des garanties suffisantes pour assurer la protection des données conformément au RGPD.
La CNIL considère que le mineur validant l'opération dans le cadre d'un smart contract, le fait pour le compte de l'entité ayant développé le smart contract.[94] Le mineur pourrait donc être assimilé au sous-traitant défini par l'art. 28 RGPD et soumis à l'autorité de son responsable.

Dans ce cas de figure, des difficultés persistent à notre sens. L'art. 28 al. 3 RGPD impose que la relation juridique entre le responsable du traitement et le sous-traitant soit encadrée par un contrat. Or, il va s'avérer compliqué de contracter avec le responsable d'une blockchain publique dans la mesure où il est souvent difficilement identifiable. De plus, il faudrait que chaque mineur prenant part à la validation de la chaîne de blocs soit partie à un contrat, devant être, de surcroît, soumis au droit européen ou à celui d'un État membre (art. 28 al. 3 RGPD). Or, les mineurs sont répartis dans le monde entier et n'ont pas nécessairement l'envie de s'obliger à ce type d'obligations. La CNIL, consciente de la complexité d'une telle construction appelle «les acteurs à avoir recours à des solutions innovantes leur permettant d'assurer une conformité avec les obligations que fait peser le RGPD sur le sous-traitant».[95]

Enfin, cette idée va directement à l'encontre du principe de la blockchain dans la mesure où elle vise à s'affranchir des règles humaines au profit du code. Rendre un utilisateur responsable du traitement signifierait faire de l'humain le responsable de la blockchain, alors que dans la philosophie de ses utilisateurs, code is law.

3. Le concept de privacy à l'opposé de la technologie blockchain

Le RGPD a introduit le privacy by design en imposant aux entreprises développant un projet, d'étudier celui-ci en relation avec la protection des données. L'UE a prolongé cette exigence en imposant aussi un privacy by default obligeant le responsable du traitement de mettre en œuvre des mesures appropriées dans le traitement des données personnelles (art. 25 RGPD).
La blockchain publique, sans autorité à sa tête ne peut remplir ces obligations, car elle est façonnée par ses utilisateurs de manière

90 POPPE/VERBIEST (Fn. 9), p. 39.
91 CNIL, Premiers éléments d'analyse de la CNIL – Blockchain, septembre 2018, p. 2.
92 NAFTALSKI/REVOL/FAUVEL (Fn. 46).
93 MARTIN-FORISSIER (Fn. 10); NAFTALSKI/REVOL/FAUVEL (Fn. 46).
94 CNIL, (Fn. 91), p. 4.
95 CNIL, (Fn. 91), p. 4.

décentralisée. En ce qui concerne la blockchain privée, les responsables l'organisant seraient inspirés de tenir compte de ces exigences au moment de la conception de leur produit afin d'être en conformité avec le RGPD.

4. Le transfert des données en dehors de l'UE

La blockchain s'affranchit des nations. En tant que système technologique, elle ne tient pas compte des limites territoriales des États. Tout mineur dans le monde peut participer à la blockchain rendant ainsi difficile l'application de règles de droit nationales ou régionales à une technologie dont ses contributeurs sont répartis sur l'ensemble du globe.[96] Par ce système, d'importantes données s'échangent à travers le monde. Or, les art. 44 ss RGPD imposent un certain nombre de conditions en cas de transfert à l'étranger, notamment une décision d'adéquation (art. 45 RGPD) et des garanties appropriées (art. 46 RGPD). Dans la blockchain publique, personne ne peut mettre en œuvre ces obligations,[97] rendant une fois de plus la blockchain publique peut aisée à encadrer juridiquement.

5. Le droit à l'effacement des données: une exigence incompatible avec la blockchain

L'art. 17 al. 1 RGPD instaure le droit à l'effacement, assimilable à un droit à l'oubli. Pareille exigence va à l'opposé du fonctionnement de la blockchain. Il n'est pas possible d'effacer une opération de la blockchain.[98] Toute opération effectuée sur celle-ci est irrémédiable. Tout au plus peut-on effacer en modifiant les données de la blockchain afin qu'elle soit de nouveau dans l'état antérieur à l'opération lui ayant été demandée.[99] Effectuer cette opération implique de paralyser l'accès à la blockchain pendant le temps de l'opération d'effacement, entraînant pour conséquence l'impossibilité de réaliser d'autres opérations.[100] Une majorité est nécessaire entre les participants de la blockchain pour pouvoir la modifier[101] entraînant ainsi un «soft fork», permettant de modifier la blockchain.

Cependant, l'art. 17 al. 2 RGPD vient tempérer les exigences imposées par l'al. 1 du même art. en imposant, «compte tenu des technologies disponibles et des coûts de mise en œuvre», au responsable du traitement de prendre les mesures appropriées pour «informer les responsables du traitement» des données personnelles traitées que la personne concernée souhaite voir supprimées. Ainsi, si un responsable du traitement était déterminé au sein de la blockchain, la limitation de l'art. 17 al. 2 RGPD pourrait se voir appliquée à la blockchain.

Une autre approche permettrait de remédier à cette incompatibilité: faire renoncer au participant à la blockchain à son droit à l'effacement.[102] Ce renoncement serait en effet justifié par rapport au but propre de la blockchain: la conservation des données.[103] Un tel renoncement semble difficile à obtenir dans une blockchain publique, du fait, une fois de plus, de l'absence d'autorité pouvant demander aux participants de renoncer à son droit à l'effacement. Dans une blockchain privée, l'autorité l'organisant pourrait facilement le faire. Si une partie s'y oppose, elle ne pourrait pas participer à la blockchain.

---

96 GRAHAM-SIEGENTHALER/FURRER (Fn. 10), nº 27.

97 NAFTALSKI/REVOL/FAUVEL (Fn. 46).

98 LEGEAIS (Fn. 87), p. 10; Rapport groupe fintech, Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché, Paris Europlace 2017 (cité: Paris Europlace), p. 81.

99 POPPE/VERBIEST (Fn. 9), p. 39.

100 Ibidem.

101 MEYER (Fn. 21).

102 PARIS EUROPLACE (Fn. 97), p. 83.

103 Ibidem.

IV. Conclusion

La blockchain est à notre sens largement incompatible avec un grand nombre des exigences posées par le RGPD. Il pourrait néanmoins être objecté et peut-être même reproché au RGPD d'ignorer une technologie aussi disruptive que la blockchain. L'incompatibilité de la blockchain publique avec le RGPD n'est cependant pas absolue, tant cette technologie est encore jeune. Le monde découvre progressivement son fonctionnement et ses fonctionnalités.

Si la blockchain n'est pas en mesure actuellement de garantir un anonymat complet de l'utilisateur et de protéger efficacement ses données, combien d'acteurs du numérique peuvent aujourd'hui s'en targuer? Sans doute peu, si l'on suit les nombreux vols de données constatés (Swisscom, Facebook, Ashley Madison, British Airways ou encore JPMorgan Chase & Co,[104] etc).

Si la blockchain privée peut se réguler et assurer une certaine conformité face aux (trop) lourdes exigences réglementaires imposées par le RGPD grâce à son caractère contractuel et par le data protection by design. Il en va autrement de la blockchain publique. Les utilisateurs de cette dernière, doivent, s'ils souhaitent la rendre conforme aux règles s'appliquant à la protection des données, consentir à d'importants efforts. Il s'agirait en effet de changer la morphologie et la philosophie de la blockchain publique qui ne se prête pas aux exigences de la protection des données.

La blockchain publique et ses soutiens, doivent ainsi, s'ils veulent devenir les garants de la protection des données et rendre la blockchain compatible au RGPD, consentir à d'importants changements dans l'essence même de la blockchain. Mais sacrifier la blockchain sur l'autel de la protection des données n'est à notre sens pas souhaitable. Céder au chant des sirènes de la technologie et renier la protection nécessaire des données l'est encore moins. Néanmoins, de tels changements, consentis ou subis, sont à l'opposé de la philosophie libertaire de la blockchain et de ses membres réticents à toute intervention étatique. Il est néanmoins loisible de s'interroger plus largement sur l'existence même de la notion de données personnelles et l'efficacité de leur protection. Il est fort probable qu'à l'avenir, la technologie blockchain prenne le dessus sur la protection des données. En effet, les règles sur la protection des données parviennent difficilement à protéger les données des citoyens. De plus, la blockchain offre une multitude de possibilités la rendant déjà incontournable. Enfin, il est fort probable que le droit ne parvienne pas à réguler cette technologie du fait de sa structure sans autorité à sa tête.

Il semblerait que la blockchain se situe aujourd'hui à un carrefour. Deux chemins apparaissent. Un premier, empruntant une certaine forme d'institutionnalisation, passant par une régulation. Cette voie dénaturerait néanmoins la philosophie de la blockchain. A l'inverse de cette première conception, un deuxième chemin existe. Celui-ci permettrait à la blockchain de conserver sa philosophie originelle de plateforme affranchie de la tutelle des États et des banques. Néanmoins ce chemin, passe par un affranchissement de la blockchain à la règle de droit et notamment à celles relatives à la protection des données.

---

104 AWP, Swisscom reconnaît le vol de données de 800'000 clients, Bilan, 7 février 2018; ISAAC MIKE/FRENKEL SHEERA, Facebook security breach exposes accounts of 50 million users, The New York Times, 28 septembre 2018; LORD NATE, A timeline of the Ashley Madison Hack, Digital Guardian, 27 juillet 2017; JOLLY JASPER, British Airways: 185'000 more passengers may have had details stolen, The Guardian, 25 octobre 2018; CROWE PORTIA, JPMorgan fell victim to the largest theft of customer data from a financial institution in US history, Business Insider, 10 novembre 2015.