Loren Jolly

La protection des droits fondamentaux des utilisateurs de FinTech : l'exemple de l'application du Règlement Général sur la Protection des Données

Abstract

The aim of this article is to highlight the different issues that one faces when trying to ensure fundamental rights of FinTech users. Data protection and especially the provisions of the General Data Protection Regulation are used as an example of the difficulties. Here, three principal issues are addressed: issues regarding the addressees of the General Data Protection Regulation's provisions, issues regarding the difference made in the General Data Protection Regulation between personal, pseudonymised and anonymised data and finally issues regarding the qualification and treatment of data available on permissionless and permissioned blockchains. Finally this article highlights the consequences that these uncertainties may have on the protection of FinTech's user's fundamental rights and the necessity to ensure legal certainty through additional guidance from the European legislator or upcoming case-law.

Zusammenfassung

Ziel des Beitrags ist es, die verschiedenen Schwierigkeiten aufzuzeigen, die einem bei dem Versuch begegnen, die Grundrechte von FinTech-Nutzern zu gewährleisten. Der Datenschutz, genauer die Regelungen der Datenschutz-Grundverordnung dienen als Beispiel für die Schwierigkeiten. Es werden hier drei Problemfelder behandelt: das Problem der Adressaten der Datenschutz-Grundverordnung, die aufgrund der durch die Datenschutz-Grundverordnung getroffenen Unterscheidung zwischen personenbezogenen, pseudonymisierten und anonymisierten Daten auftretenden Probleme und schließlich die Probleme der Einordnung verfügbarer Daten auf öffentlichen und zugangsbeschränkten Blockchains. Schließlich zeigt der Beitrag die möglichen Folgen dieser Unsicherheiten für den Schutz der Grundrechte der FinTech-Nutzer auf sowie die Notwendigkeit, die Rechtssicherheit durch zusätzliche Anleitungen des europäischen Gesetzgebers oder zukünftige Rechtsprechung zu gewährleisten.

Introduction

Le droit fondamental à la protection des données dans l'Union européenne

La protection et la promotion des droits fondamentaux au sein de l'Union européenne ont fait l'objet d'un un long processus. La Cour de Justice de l'Union européenne (la « **CJUE** »), déjà en 1970, considérait que sa jurisprudence respectait les droits fondamentaux comme faisant partie des principes généraux inspirés par les traditions constitutionnelles communes des Etats membres et protégés par la CJUE. Elle con-

KritV 1/2018, DOI: 10.5771/2193-7869-2018-1-68

sidérait aussi que les droits fondamentaux devaient être assurés au sein de la communauté européenne[1] et les plaçait au sein du cadre de la structure et des objectifs de l'Union européenne. Dès lors, avant même d'être introduits dans le droit positif européen, la protection des droits fondamentaux était déjà assurée au niveau européen en tant que principes généraux du droit communautaire inspirés des constitutions des Etats membres et de la Convention européenne des Droits de l'Homme (la « **CEDH** »). Les institutions de l'Union européenne partageaient cet avis. En effet, en 1977, le Parlement européen, le Conseil et la Commission, dans une déclaration commune mettaient en avant l'importance primordiale du respect des droits fondamentaux dans l'exercice de leurs pouvoirs.[2]

Néanmoins, le fait que la protection des droits fondamentaux au sein de l'Union européenne était uniquement basée sur des principes généraux et non pas assurée en droit positif communautaire ne permettait pas d'assurer la sécurité juridique. En effet, puisqu'il n'y avait pas de base légale pour la protection des droits fondamentaux en droit européen, ces droits étaient difficilement prévisibles et les citoyens européens manquaient de sécurité juridique.[3]

C'est pourquoi les traités ont petit à petit codifié les droits fondamentaux de manière à leur donner une valeur juridique équivalente à celle des traités. Premièrement, le Traité d'Amsterdam avait pour objectif en 1999 de développer un espace de liberté, de sécurité et de justice au sein de l'Union.[4] Le Traité d'Amsterdam introduisait une obligation de protection des données à laquelle étaient soumises les institutions européennes et autres organes européens.[5] Cependant, c'est le Traité de Lisbonne qui a donné une réelle valeur à la protection des droits fondamentaux au sein de l'Union européenne. Premièrement, le préambule du Traité sur l'Union européenne (le « **TUE** ») rappelle l' « attachement aux principes de la liberté, de la démocratie et du respect des droits de l'homme et des libertés fondamentales et de l'État de droit. »[6] Deuxièmement, il reconnaît à la Charte des droits fondamentaux de l'Union européenne la même valeur juridique que les Traités.[7]

Cet article se concentre sur l'un des droits fondamentaux qui est particulièrement protégé au sein de l'Union européenne à cause de l'importance majeure qu'il a vis-à-vis du droit à une vie privée:[8] le droit à la protection des données. Celui-ci n'est pas

1 CJUE, Internationale Handelsgesellschaft c. Einfuhr und Vorratsstelle Getreide, 11/70, 17 décembre 1970, p. 1034.

2 Parlement européen, Conseil, Commission, Déclaration commune, no. C103-1, 27 avril 1977.

3 Parlement européen, Francesca Ferraro, Jesùs Carmona, Les droits fondamentaux dans l'Union européenne, Le rôle de la Charte après le traité de Lisbonne, Service de recherche du Parlement européen, mars 2015, p. 7.

4 Traité d'Amsterdam amendant le Traité sur l'union européenne, le Traité établissant les communautés européennes et certains actes connexes, 1977, considérant 10 tel que modifié et art. B tel que modifié.

5 *Idem*, art. 213(b) tel que modifié.

6 TFUE, 26 octobre 2012, préambule.

7 *Idem*, art. 6(1).

8 Conseil de l'Europe, Ursula Kilkelly, The right to respect for private and family life, A guide to the implementation of Article 8 of the European Convention on Human Rights, Human rights handbooks, no. 1, 2001, p. 40.

seulement garanti par l'article 8(1) de la Charte des droits fondamentaux mais aussi par l'article 16(1) du Traité sur le fonctionnement de l'Union européenne (le « **TFUE** »). L'article 16(2) du TFUE est la base légale pour les instruments de droit dérivé sur la protection des données personnelles.[9] Cet article se focalisera sur le nouvel instrument qui harmonise la protection des données au sein de l'Union : le Règlement Général sur la Protection des Données (le « **RGPD** »).[10] Le RGPD remplacera la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (la « **Directive 95/46** »)[11] à partir de mai 2018 afin d'assurer un niveau équivalent de protection des personnes physiques et le libre flux des données à caractère personnel dans l'ensemble de l'Union.[12]

Les mesures pour assurer la protection des données dans le RGPD

Les dispositions du RGPD incluent deux différentes manières d'établir un cadre protecteur des données personnelles. Premièrement, le RGPD met en place des mesures de contrôle individuel pour les personnes concernées par le traitement (dorénavant, les « **personnes concernées** »). Ces mesures doivent être comprises comme donnant la possibilité à la personne concernée de déterminer par elle-même quand, comment et dans quelles mesures des informations la concernant peuvent être communiquées à des tiers.[13] Il s'agit donc de donner des droits aux individus, la possibilité de faire eux-mêmes appliquer leur droit à la protection des données ainsi qu'un moyen d'exercer un certain contrôle sur les données les concernant. Cette théorie a été soutenue par de nombreux universitaires[14] et est communément reconnue comme la solution aux possibles ingérences dans le droit à la vie privée découlant de la perte de contrôle des

9 TFUE, 26 octobre 2012, art. 16(2), «Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les Etats membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes ».

10 Parlement européen, Conseil, Règlement 2016/679 (EU) 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, 27 avril 2016.

11 Parlement européen, Conseil, Directive 95/46/EC relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 24 octobre 1995.

12 RGPD, considérant 170.

13 Robert Baud, Marius Fieschi, Pierre Le Beux, Patrick Ruch, The new navigators: from professionals to patients, no. 95, Studies in Health Technology and Informatics, IOS Press, p. 174.

14 Voir par exemple Charles Fried, Privacy, Information and Technology, ASPEN Publishers, 2006, p. 39, « privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves » et William Parent, Privacy, Morality and the Law, Philosophy and Public Affairs, 12: 269–88, 1983, p. 270, qui reconnaît l'importance du choix et du contrôle à propos de « facts that most persons in a given society choose not to reveal about themselves. ».

individus quant aux données les concernant.[15] Un certain nombre de mesures basées sur cette théorie peuvent être trouvées dans le RGPD. Par exemple, le RGPD donne aux personnes concernées la possibilité de contrôler leurs données en exigeant l'obtention de leur consentement avant que le traitement n'ait lieu ou encore en donnant aux personnes concernées un certain nombre de droits spécifiques qu'ils peuvent invoquer (il s'agit par exemple du droit d'accès aux données, le droit à la rectification des données ou encore le droit à l'oubli). Cette théorie a été perçue comme un moyen de permettre l'autonomisation et l'autodétermination de la personne concernée confrontée au traitement massif de données lié au développement technologique et à l'ère du Big data.

Deuxièmement, le RGPD contient des dispositions visant à assurer la régulation des risques. Le développement de ce type de mesures vient de l'évolution de la technologie et est la conséquence du fait que le contrôle des individus sur les données personnelles les concernant est pratiquement infaisable dans une ère où les données sont omniprésentes.[16] Ces mesures visent à imposer des obligations sur les responsables du traitement et sous-traitants de manière à ce qu'ils agissent de manière juste et respectueuse des personnes concernées. Il s'agit donc d'assurer que, même si les individus n'exercent pas leurs droits, ils recevront malgré tout un niveau adéquat de protection des données. Ce type de mesures est bien présent dans les dispositions du RGPD qui impose des obligations aux responsables du traitement et sous-traitants comme celle de mettre en place des mesures techniques et organisationnelles pour assurer la sécurité du traitement, la protection des données dès la conception et par défaut ou encore l'obligation de désigner un délégué à la protection des données.

Dès lors, en général, il peut être considéré que le RGPD propose un niveau global de protection des droits fondamentaux des personnes concernées puisqu'il ne leur donne pas seulement la possibilité d'exercer un contrôle sur les données les concernant, mais il impose aussi des obligations aux responsables des traitements et sous-traitants.

De nouvelles interrogations soulevées par le développement des FinTech

Malgré le fait que le RGPD sera applicable à partir de mai 2018 seulement, il a été initialement proposé par la Commission européenne en 2012,[17] à un moment où certaines technologies qui sont aujourd'hui un sujet de préoccupation étaient encore à un stade très précoce de leur développement. Il peut s'agir d'une raison pour laquelle le RGPD ne mentionne pas ces technologies et pose ainsi un certain nombre d'interrogations lorsque l'on tente d'appliquer ses dispositions aux acteurs proposant des services fondés sur l'utilisation de ces nouvelles technologies dans le secteur de la finance ou dans tout autre secteur.

15 Rayan Calo, The boundaries of privacy harm, Indiana law journal, no. 86, 2011, p.1134, qui décrit une atteinte à la vie privée comme « the loss of control over information about oneself or one's attributes. ».

16 Christophe Lazaro, Daniel Le Métayer, The control over personal data: True remedy or fairy tale?, Project-Teams Privatics, Research Report no. 881, 13 avril 2015, p. 23.

17 Commission européenne, proposition de règlement 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 (Règlement Général sur la Protection des Données), 25 janvier 2012.

Grâce au développement des FinTech (concept devant être compris comme une activité financière rendue possible par de nouvelles technologies ou fournie par l'intermédiaire de ces technologies, touchant l'ensemble du secteur financier dans toutes ses composantes, des opérations bancaires aux assurances, en passant par les fonds de pension, le conseil en investissement, les services de paiement et les infrastructures de marchés),[18] les utilisateurs ont la possibilité de se voir proposer des services plus efficaces, plus personnalisés et moins coûteux. Les FinTech peuvent aussi être un instrument permettant l'inclusion financière[19] et pourraient donc proposer des services aux individus qui ne peuvent pas se permettre de passer par des services traditionnels. C'est pourquoi il est dans l'intérêt des utilisateurs de voir les FinTech se développer. La réglementation doit donc s'appliquer dans l'intérêt des consommateurs et rester technologiquement neutre. Cela signifie que les services financiers utilisant des nouveaux moyens technologiques pour proposer leurs services ne devraient pas être considérés comme risqués uniquement parce qu'ils utilisent ces technologies. C'est pourquoi, il faudrait sortir des conflits traditionnels qui existent entre les juristes d'une part et les techniciens d'autre part : le droit ne devrait pas entrer en conflit avec la technologie mais au contraire devrait la soutenir de manière à développer son utilisation et offrir une protection juridique adéquate aux utilisateurs de services fondés sur ces technologies.

La législation et la réglementation devraient s'adapter à l'innovation et un juste équilibre devrait être trouvé de manière à pouvoir protéger les consommateurs et, en même temps, encourager l'innovation. Le Parlement européen rappelle que les prestataires de services proposant le même type d'activités ne doivent pas être réglementés différemment, simplement à cause de la technologie sous-jacente qu'ils utilisent.[20] Finalement la législation et la réglementation doivent rester dans l'intérêt des consommateurs puisqu'ils sont l'élément moteur derrière le développement des FinTech.[21]

En termes de protection des données, il y a un fort besoin de mettre en place une application technologiquement neutre du RGPD de manière à développer et encourager une Union européenne innovatrice en termes d'industrie financière.[22] Conjointement, un niveau équivalent de protection des données doit être garanti lorsqu'il est fait usage de ces nouvelles technologies. Ainsi, les consommateurs seront plus enclins à utiliser de nouveaux types de services comme ceux proposés par les FinTech. Cela aura aussi certainement une influence sur le développement de l'Union européenne en tant que place d'innovation et favorable aux nouveaux arrivants sur le marché.

FinTech, sécurité juridique et respect de l'Etat de droit

Non seulement un niveau de protection des données équivalent à celui lorsque des services traditionnels sont utilisés doit être garanti, mais aussi la prévisibilité de l'application des règles relatives à la protection des données aux FinTech doit être assurée.

18 Parlement européen, Commission des affaires économiques et monétaires, Rapport sur la technologie financière: influence de la technologie sur l'avenir du secteur financier, (2016/2243(INI)), 28 avril 2017, p. 4.
19 *Idem*, p. 5.
20 *Idem*, p. 8.
21 *Idem*, p. 10.
22 *Idem*, p. 10.

En effet, le respect de l'Etat de droit et de ses principes sous-jacents (entre autre les principes de légalité, de sécurité juridique et la prohibition de l'arbitraire)[23] vise à assurer la prévisibilité du droit. De plus, il vise à assurer le respect des droits fondamentaux.[24] L'Etat de droit constitue une des valeurs sur laquelle est basée l'Union européenne[25] et doit en toutes circonstances être respecté et assuré.

L'essence même de l'Etat de droit étant l'implémentation de principes visant à assurer la prévisibilité du droit,[26] les incertitudes mentionnées ci-dessus quant à la protection des droits fondamentaux lorsqu'il est fait usage de nouveaux moyens technologiques, peuvent avoir des conséquences négatives sur la sécurité juridique. Le Parlement européen considère que l'usage de FinTech ne doit pas diminuer la protection des consommateurs et leur droit à une protection de leurs données.[27] Cependant, le manque de sécurité juridique restera une préoccupation jusqu'à ce que quelques problèmes soient résolus par le législateur européen et de manière à ce que les personnes concernées reçoivent exactement le même niveau de protection des données indépendamment du fait que le responsable du traitement ou ses sous-traitants utilisent des nouveaux moyens technologiques ou des moyens plus traditionnels afin de traiter les données dont ils disposent.

Cet article se concentrera sur l'analyse de la réalisation du droit fondamental à la protection des données lorsque des moyens technologiques avancés sont utilisés : les FinTech et la Blockchain. Il s'agira d'évaluer les problèmes persistants que rencontre l'application du RGPD à ces nouveaux acteurs et les instruments et moyens qui pourraient permettre de les résoudre. Le but de cet article sera de mettre en évidence les difficultés qui persistent lorsque l'on tente d'appliquer le RGPD aux FinTech et donc les obstacles empêchant une protection efficace des droits fondamentaux des consommateurs. Pour finir, cet article visera à analyser les conséquences de ces problèmes persistants sur la sécurité juridique et sur l'exercice du droit à la protection des données des personnes concernées.

Afin de répondre à ces questions, les interrogations concernant les destinataires des obligations prévues par le RGPD seront analysées (Partie I), ensuite les enjeux liés à la distinction faite par le RGPD entre les données personnelles, les informations anonymes et les données pseudonymisées seront évoqués (Partie II), les interrogations quant à la qualification et le traitement de données sur des blockchains publiques et privées seront mises en exergue (Partie III) et la dernière partie sera consacrée aux conséquences que ces interrogations et incertitudes peuvent avoir sur la protection des droits fondamentaux des consommateurs (Partie IV).

23 Commission européenne, Communication de la Commission au Parlement européen et au Conseil, Un nouveau cadre de l'UE pour renforcer l'Etat de droit, 19 mars 2014, p. 4.

24 Conseil de l'Union européenne, Conseil 'Justice et affaires intérieures', Doc. 10168/13, 29 mai 2013.

25 TUE, art. 2.

26 Jeremy Waldron, The concept and the rule of law, New York University school of law, public law & legal theory research paper series working paper no. 08-50, novembre 2008, p. 60.

27 Parlement européen, Commission des affaires économiques et monétaires, Rapport sur la technologie financière: influence de la technologie sur l'avenir du secteur financier, (2016/2243(INI)), 28 avril 2017, p. 10 et 14.

I. Interrogations concernant les destinataires des obligations

D'après la Directive 95/46, uniquement le responsable du traitement était sujet à des obligations en termes de protection des données. Le RGPD a introduit de nouvelles règles qui ne contraignent pas seulement les responsables du traitement mais aussi leurs sous-traitants alors qu'ils étaient auparavant simplement soumis à leurs obligations contractuelles.[28] Avec l'application du RGPD, ils partageront la responsabilité pour non-respect de ses dispositions et les personnes concernées pourront invoquer leur droit à un recours juridictionnel effectif à l'encontre du responsable du traitement mais aussi à l'encontre de ses sous-traitants.[29]

Un responsable du traitement est défini comme l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.[30] Un sous-traitant doit être entendu comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.[31] Le traitement n'inclut pas seulement l'analyse et le traitement de données mais aussi la collecte, l'enregistrement, la conservation ou le fait de mettre à disposition des données.[32] Dès lors, le traitement inclut des types d'activités très différents : des activités très actives et d'autres plus passives qui peuvent être exécutées par des services informatiques hébergés plus communément appelés services de cloud computing. Dans cette première partie, il s'agira de démontrer que les définitions de responsable du traitement et sous-traitant données par le RGPD peuvent être remises en question. Pour ce faire, les services de cloud computing seront utilisés comme exemple (A). Ensuite, il s'agira d'envisager l'application des dispositions du RGPD à des acteurs sur une blockchain et la manière dont cela pourrait être fait (B).

A. L'exemple des services de cloud computing

L'objectif du RGPD est de prévenir l'accès non autorisé, l'utilisation ou la divulgation de données à caractère personnel.[33] Cela n'est possible que lorsque le responsable du traitement ou le sous-traitant a accès au contenu des données, c'est-à-dire lorsqu'il a accès à des données personnelles intelligibles. Il faudrait donc faire la différence entre, d'une part, une situation où seulement le responsable du traitement a accès à des données intelligibles et, d'autre part, une situation où cet accès est partagé avec le sous-traitant. Si cela n'est pas fait, alors le sous-traitant pourra être tenu pour responsable d'avoir traité des données personnelles sans respecter les dispositions du RGPD alors qu'il n'avait pas conscience qu'il s'agissait de données personnelles étant donné qu'il n'avait pas accès au contenu des données qu'il traitait (par exemple parce que sa

28 Directive 95/46, art. 17(3) et 23(1).
29 RGPD, art. 79.
30 *Idem*, art. 4(7).
31 *Idem*, art. 4(8).
32 *Idem*, art. 4(2).
33 RGPD, art. 4(12) et Deven Desai, Beyond Location: Data Security in the 21st Century, Law and Technology, vol. 56, no. 1, janvier 2013, p. 34.

tache se limitait à conserver ou rendre disponible ces données pour le responsable du traitement).

Cela peut être un enjeu considérable pour les acteurs proposant certains types de services. Par exemple, les services de cloud computing[34] pourraient devenir réticents à autoriser certains responsables de traitement utiliser leurs services pour effectuer du traitement de données parce qu'ils pourraient partager la responsabilité en cas de non-respect des dispositions du RGPD.

Cela aura probablement des conséquences sur la manière dont les contrats de services seront négociés et rédigés à l'avenir. Premièrement, les contrats de services incluant comme activité le traitement de données personnelles devront être revus en accord avec les exigences de l'article 28(36)[35] de manière à être en conformité avec le RGPD. Les négociations pourront devenir plus difficiles étant donné que les prestataires de services deviendront plus attentifs aux activités de leurs clients et cette tendance sera d'autant plus importante pour les sous-traitants implantés en dehors de l'Union européenne puisqu'ils pourront être réticents à se voir appliquer un nombre aussi important de nouvelles obligations. En effet, le champ d'application territorial du RGPD est plus large que celui de la Directive 95/46 puisqu'il inclut le traitement effectué par des responsables ou sous-traitants non établis sur le territoire de l'Union européenne mais ciblant des individus se trouvant dans l'Union européenne et donc, soumis aux droits et obligations prévus par le RGPD.[36]

Une solution à cette interrogation pourrait être trouvée dans le RGPD lui-même puisque celui-ci prévoit, dans son article 2(4), qu'il s'applique sans préjudice de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (la « **Directive sur le commerce électronique** »), notamment de ses articles relatifs à la responsabilité des prestataires de services intermédiaires. Les articles auxquels le RGPD fait référence, prévoient des exonérations de responsabilité pour les intermédiaires.

Néanmoins, il est nécessaire de clarifier ce que cela signifie en pratique. Cela pourrait signifier que le champ d'application du RGPD est limité et n'outrepasse pas les dispositions sur l'exonération de responsabilité prévues par la Directive sur le commerce électronique,[37] ou cela peut aussi être un moyen d'accepter le fait que ces mesures d'exonération de responsabilité prévues par la Directive sur le commerce électronique soient aussi applicables aux questions de protection des données dans certains cas.[38] Il pourrait donc être entendu que les exonérations de responsabilité prévu-

34 Voir définition de cloud computing dans: Groupe de travail Article 29 sur la Protection des Données, Opinion 05/2012 on Cloud Computing, p.4, « a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. ».

35 RGPD, art. 28(36) qui mentionne les obligations qu'un responsable de traitement de données personnelles doit respecter.

36 *Idem*, art. 3.

37 Jaani Riordan, The liability of Internet intermediaries, Oxford, [10.261], 2016.

38 Kuan Hon, Presentation on Cloud Security under the EU Data Protection Directive and draft General Data Protection Regulation, ENISA EU28 Cloud Security Conference, 16 juin 2015.

es par la Directive sur le commerce électronique puissent être appliquées aux prestataires de services intermédiaires pour des questions de protection des données lorsque le traitement est effectué par leurs clients (dès lors, les intermédiaires devraient être considérés comme des intermédiaires), mais la responsabilité reposerait toujours sur les prestataires de services lorsqu'il s'agira de leur propre traitement de données personnelles (ici, les prestataires devraient alors être considérés comme des responsables du traitement).[39]

Si l'on considère que la deuxième option est en effet l'approche qui était envisagée par le législateur européen, alors cela pourrait résoudre l'interrogation que nous avons soulevée dans ce paragraphe. Afin d'être consistant, l'article 5(b) de la Directive sur le commerce électronique, qui pour l'instant exclut de son champ d'application les questions de protection des données, devrait être revu et amendé. Aussi, il devrait être clairement déterminé pour quel type d'activités un prestataire de service doit être considéré comme un intermédiaire ou comme un responsable de traitement. L'accès et le contrôle de données personnelles intelligibles devraient devenir les conditions préalables à la responsabilité des services de cloud computing de façon à ce que le RGPD reste technologiquement neutre.[40] Dès lors, les exonérations de responsabilité prévues par la Directive sur le commerce électronique deviendraient applicables aux questions de protection des données et les prestataires de services intermédiaires pourraient en bénéficier, en fonction de leurs activités et du rôle qu'ils jouent dans le traitement des données. Cela pourrait avoir des conséquences positives sur l'innovation puisque les services de cloud computing pourraient alors être moins réticents à allouer leurs services pour des traitements de données concernant des personnes localisées sur le territoire de l'Union européenne.

B. L'exemple des blockchains publiques

Cependant, les services de cloud computing ne sont pas les seuls acteurs qui rendent l'application des dispositions du RGPD problématique. L'une des principales composantes des FinTech est la technologie Blockchain. D'après le rapport du Parlement européen du 28 avril 2017, déjà cité ci-dessus et considérant que les FinTech ne doivent pas diminuer le niveau de protection des données de leurs utilisateurs; le RGPD devrait être applicable aux blockchains.

Néanmoins, il est particulièrement difficile de déterminer sur une blockchain, à qui les obligations prévues par le RGPD devraient être imposées et qui devrait être considéré comme responsable en cas de violation. A première vue, il est difficile de trouver un responsable de traitement approprié sur une blockchain publique. Néanmoins, il y a un certain nombre d'acteurs sur qui la responsabilité pourrait éventuellement reposer : cela pourrait par exemple être le créateur du système lorsque celui-ci est connu (ce qui n'est par exemple pas le cas pour la blockchain Bitcoin), les différents nœuds

39 Bird&Bird, Ruth Boardman, James Mullock, Ariane Mole, Guide to the General Data Protection Regulation, mai 2017, page 4.

40 Kuan Hon, Eleni Kosta, Christopher Millard, Dimitra Stefanatou, Cloud accountability: the likely impact of the proposed EU Data Protection Regulation, Tilburg law school legal studies research paper series, no. 07/2014, 7 mars 2014, p. 21 et 46.

de la blockchain ou encore les mineurs qui contribuent au fonctionnement du système. Le législateur pourrait aussi décider de réguler les acteurs qui agissent autour de la blockchain et contribuent à rendre l'utilisation des blockchains plus facile pour les utilisateurs non-techniciens en construisant un pont entre les cryptomonnaies et les monnaies ayant cours légal. Cette solution a d'ailleurs été d'ores et déjà choisie dans le contexte de la lutte contre le blanchiment de capitaux et le financement du terrorisme lorsque le Parlement européen et la Commission ont annoncé que les dispositions de la Directive relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme[41] devraient s'appliquer aux fournisseurs de services de change de cryptomonnaies et aux fournisseurs de portefeuilles de stockage.[42] Néanmoins, cela n'a pas été encore résolu par le législateur dans le cadre de la protection des données et dès lors, certaines interrogations persistent quant à la manière d'appliquer effectivement et efficacement le RGPD aux blockchains publiques. En attendant que cette question soit abordée par le législateur européen, il restera impossible d'identifier un responsable du traitement qui pourrait être considéré responsable si une violation se produit.

En résumé, des indications supplémentaires sont nécessaires concernant les destinataires des dispositions du RGPD : la notion de sous-traitant devrait être détaillée de manière à ce que le rôle des prestataires de service ainsi que leurs obligations soient clairs. De plus, des indications supplémentaires sont nécessaires concernant l'application des dispositions du RGPD aux blockchains publiques puisqu'il est particulièrement difficile de déterminer avec certitude qui doit être défini comme responsable du traitement (ou sous-traitant) dans un système aussi décentralisé qu'une blockchain.

II. Interrogations relatives à la distinction faite par le RGPD entre les données personnelles, les informations anonymes et les données pseudonymisées

Cette partie visera à expliquer que les strictes distinctions faites par le RGPD entre les données personnelles d'une part et les données anonymes d'autre part ne reflètent pas précisément la réalité technologique de par le fait que la technologie évolue à une vitesse particulièrement rapide (A). Finalement, la qualification et le traitement choisi par le RGPD pour s'appliquer aux données pseudonymisées seront aussi remis en question avec un raisonnement fondé sur l'efficacité des mesures (B).

41 Parlement européen, Conseil, Directive (EU) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, 20 mai 2015.

42 Parlement européen, Rapport sur la proposition de Directive du Parlement européen et du Conseil modifiant la Directive (UE) n° 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et la directive 2009/101/CE (COM(2016)0450 – C8-0265/2016 – 2016/0208(COD)), 9 mars 2017, considérant 6, et Commission européenne, Communiqué de presse, La Commission présente un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, 2 février 2016.

A. Données personnelles vs. données anonymes

1. En théorie

Les données personnelles, entrant dans le champ d'application du RGPD, doivent être entendues comme « toute information se rapportant à une personne physique identifiée ou identifiable […]. »[43] Des données peuvent être personnelles de par leur contenu (1), de par l'objectif poursuivi (2), ou de par le résultat du traitement (3).[44] Cela signifie que les données peuvent se rapporter à une personne physique identifiée ou identifiable de trois manières différentes :

1. une donnée est personnelle de par son contenu lorsque, peu importe l'objectif du traitement de celle-ci, elle sera personnelle quoi qu'il en soit car la donnée en elle-même est personnelle;
2. une donnée est personnelle de par l'objectif poursuivi lorsqu'elle est utilisée avec pour objectif d'évaluer, de traiter d'une certaine manière ou d'influencer la situation ou le comportement d'un individu; et
3. une donnée est personnelle de par le résultat du traitement lorsque la donnée peut avoir un impact sur une certaine personne, en fonction du contexte du traitement et ce, même s'il ne s'agissait pas de l'objectif du traitement.[45]

C'est pourquoi, pour déterminer si une donnée doit être considérée comme étant à caractère personnel et donc entrant dans le champ d'application du RGPD, le contexte de l'analyse de cette donnée doit être pris en compte. Il est non seulement nécessaire d'évaluer ce qui va être fait de la donnée en question mais il faut aussi prendre en compte l'éventualité qu'elle puisse être combinée avec d'autres données. Une donnée peut d'ailleurs être considérée comme personnelle lorsqu'un certain usage en est fait, puis être considérée comme non-personnelle dans un contexte différent, lors d'une analyse postérieure. La classification des données comme personnelles ou bien non-personnelles est toujours dépendante du contexte du traitement qu'il en est fait.[46]

Enfin, des données ayant subi un processus d'anonymisation de manière à ce que la personne concernée n'est plus identifiable et les données ne se rapportent plus à une personne physique identifiée ou identifiable n'entrent pas dans le champ d'application du RGPD.[47] Des techniques d'anonymisation efficaces et solides doivent assurer que :

1. des données concernant un même individu ne peuvent pas être isolées à l'intérieur d'une base de données;
2. deux données ou plus concernant un individu ne peuvent être mises en relation; et
3. des informations à propos d'un individu ne peuvent être devinées.[48]

---

43 RGPD, art. 4(1).
44 Groupe de travail Article 29 sur la protection des données, Opinion 4/2007 on the concept of Personal Data, 20 juin 2007, p.10.
45 *Idem*, p. 10 et 11.
46 *Idem*, p. 25.
47 RGPD, considérant 26.
48 Groupe de travail Article 29 sur la protection des données, Opinion 05/2014 on Anonymisation Techniques, 10 avril 2014, p. 3.

2. En pratique :

Le monde dans lequel nous vivons est en constant développement et la technologie progresse à une vitesse très importante. Dès lors, grâce à des moyens techniques particulièrement avancés et efficaces, des données supposées être anonymes peuvent éventuellement plus tard être reliées à l'identité de la personne concernée. D'ailleurs, d'après la doctrine scientifique, il y a toujours un risque de ré-identification nonobstant les techniques ayant été mises en place pour anonymiser des données.[49] Il y a de moins en moins de données qui peuvent, dans tous les cas, être considérées comme anonymes[50] et finalement la frontière entre donnée personnelle d'une part et donnée anonyme d'autre part peut varier très rapidement selon les moyens techniques disponibles. C'est pourquoi, le fait qu'une donnée entre ou pas dans le champ d'application du RGPD ne dépend pas seulement du contexte du traitement (comme nous l'avons vu en théorie), mais dépend aussi des moyens technologiques disponibles au moment du traitement.

Le risque de ré-identification a été pris en compte par le groupe de travail Article 29 sur la protection des données qui considère que le processus d'anonymisation ne doit pas être considéré comme un exercice unique puisque les déductions qui peuvent être faites à partir de données dépendent du contexte du traitement.[51] Une évaluation des risques doit être faite de manière continue de façon à ce qu'il n'y ait plus une frontière stricte entre les données anonymes et les données personnelles mais au contraire une frontière trouble qui pourrait être traversée à tout moment lorsque les données ne satisfont plus les conditions pour être traitées comme anonymes et dès lors, ne devraient plus bénéficier d'une exonération de conformité avec les dispositions du RGPD.

C'est pourquoi, une proposition adéquate serait de mettre en place une approche basée sur l'évaluation des risques des processus d'anonymisation qui inclurait une évaluation au cas par cas des faits de manière à déterminer si les données anonymes incluent à un certain moment d'importants risques de déduction d'informations à partir des données.[52] Cela devrait être fait de manière continue pour que les personnes concernées par le traitement bénéficient d'un niveau de protection des données adéquat même lorsque la technologie disponible ou les risques de déduction augmentent et quand les données sont mises en relation avec d'autres bases de données.

49 Sophie Stalla-Bourdillon, Alison Knight, Anonymous data v. personal data – a false debate: an EU perspective on anonymisation, pseudonymisation and personal data, Southampton Law School, mars 2017.

50 Paul Ohm, Broken promises of privacy: responding to the surprising failure of anonymisation, 57 UCLA L. REV. 1701, 1744, 2010.

51 Groupe de travail Article 29 sur la protection des données, Opinion 05/2014 on Anonymisation Techniques, 10 avril 2014, p. 4.

52 Sophie Stalla-Bourdillon, Alison Knight, Anonymous data v. personal data – a false debate: an EU perspective on anonymisation, pseudonymisation and personal data, Southampton Law School, mars 2017.

B. Qualification et traitement des données pseudonymisées

D'après le groupe de travail Article 29 sur la protection des données, les données pseudonymisées n'empêchent pas :

1. les données concernant un individu unique d'être isolées;
2. deux données ou plus concernant un même individu d'être mises en relation; et
3. des informations concernant un individu d'être déduites.[53]

C'est pourquoi, les données pseudonymes devraient être considérées comme des données personnelles. C'est aussi la décision prise par le législateur européen qui a décidé d'inclure les données pseudonymisées dans la définition des données personnelles et donc de les considérer comme entrant dans le champ d'application du RGPD.[54] Les processus de pseudonymisation sont néanmoins encouragés par le RGPD. Premièrement, ils sont considérés comme l'une des mesures techniques et organisationnelles adéquates à mettre en place de manière à instaurer un mécanisme efficace de protection des données dès la conception et par défaut.[55] Deuxièmement, ils sont cités comme exemples des mesures techniques et organisationnelles que les responsables du traitement et sous-traitants devraient mettre en place de manière à assurer un niveau de sécurité approprié et prévenir les accès non-autorisés ou les utilisations non-autorisées de données personnelles.[56]

Il est clair que la pseudonymisation permet de réduire les risques de mise en relation de données personnelles avec l'identité de la personne concernée. C'est la raison pour laquelle le RGPD encourage la pseudonymisation comme mesure technique et organisationnelle appropriée pour assurer la sécurité des données et le droit à la vie privée de la personne concernée.

Néanmoins, même si l'on comprend que les risques qu'impliquent les données pseudonymisées sont largement moindres par rapport aux risques qu'impliquent les données non-pseudonymisées, les données pseudonymisées sont loin d'être inclues dans la définition des données anonymes. D'après le RGPD, les données pseudonymisées ne sont pas considérées comme une catégorie spécifique de données. Une possible incitation pour les responsables du traitement et les sous-traitants d'introduire des mesures de pseudonymisation pourrait être d'accorder aux données pseudonymisées un traitement spécial.[57] Dès lors, il faut se demander si l'incitation à mettre en place des techniques de pseudonymisation des données traitées sera suffisante pour les responsables du traitement et les sous-traitants et donc si elle sera efficace.

Une solution à cela pourrait éventuellement être trouvée dans le RGPD lui-même mais dépendra de la jurisprudence à venir. Le RGPD prévoit l'adhérence à des codes

53 Groupe de travail Article 29 sur la protection des données, Opinion 05/2014 on Anonymisation Techniques, 10 avril 2014, p. 21, et Opinion 8/2014 on the Recent Developments on the Internet of Things, 16 septembre 2014, p.11.

54 RGPD, considérant 26.

55 RGPD, art. 25.

56 RGPD, art. 32.

57 Kuan Hon, Eleni Kosta, Christopher Millard, Dimitra Stefanatou, Cloud accountability: the likely impact of the proposed EU Data Protection Regulation, Tilburg law school legal studies research paper series, no. 07/2014, 7 mars 2014, p. 12 et 45.

de conduite approuvés afin de contribuer à la correcte application du RGPD[58] ainsi que l'adhérence à des mécanismes de certification afin de démontrer la conformité avec les dispositions du RGPD.[59] L'adhérence à ce type d'instruments pourrait être utilisée comme un moyen de démontrer la conformité avec les obligations de mise en place de mesures techniques et organisationnelles appropriées pour assurer un niveau adéquat de sécurité des données.[60] De plus, en cas de violation des dispositions du RGPD, lorsqu'une sanction doit être imposée, l'adhérence à un code de conduite ou à un mécanisme de certification devrait être prise en compte.[61] Ainsi, même si l'adhérence à un code de conduite approuvé ou à un mécanisme de certification ne prouve pas la conformité avec les dispositions du RGPD, cela pourrait être entendu comme un souhait concret de conformité qui devrait alors être pris en compte lorsqu'une décision relative à de possibles sanctions à imposer à des responsables du traitement ou sous-traitants n'ayant pas respecté leurs obligations doit être prise. Puisque la pseudonymisation des données est l'un des critères pris en compte par les codes de conduite approuvés,[62] l'adhérence à l'un d'entre eux présupposera probablement que des techniques de pseudonymisation adéquates ont été mises en place durant le traitement. Finalement, l'adhérence à des codes de conduite ou mécanismes de certification pourrait devenir une incitation à la mise en place de techniques de pseudonymisation s'il s'avère que cela est finalement pris en compte par les juges comme une présomption de conformité ou, au moins, une présomption d'une volonté d'être en conformité et qui permettrait aux responsables du traitement et sous-traitant n'ayant pas entièrement respecté leurs obligations de bénéficier de sanctions revues à la baisse.

Pour conclure cette partie, le traitement des données anonymes devrait être révisé. Le risque de ré-identification devrait être pris en compte et une analyse des données devrait être faite de manière continue afin de décider si elles doivent être considérées comme personnelles ou anonymes. De plus, les techniques de pseudonymisation devraient être prises en compte par les juges de façon à ce que les responsables du traitement et leurs sous-traitants aient de fortes incitations à introduire ce type de mesures.

III. La qualification des données disponibles sur une blockchain publique

Cette partie visera à mettre en évidence les difficultés rencontrées lorsque l'on tente d'appliquer le RGPD aux services qui fonctionnent via l'utilisation d'une blockchain. Même si la technologie Blockchain est souvent vue comme un système favorable à la protection de la vie privée (A), elle inclut néanmoins des risques de déduction d'informations (B) et dès lors, des risques pour la vie privée des utilisateurs (C). Le quatrième paragraphe visera à montrer que la définition de pseudonymisation proposée par le RGPD n'est pas vraiment adéquate pour aborder le cas des blockchains (D) et

58 RGPD, art. 40.
59 *Idem*, art. 42.
60 *Idem*, art. 32(3).
61 *Idem*, considérant 148 et art. 83(2)(j).
62 *Idem*, art. 40(2)(b).

le dernier paragraphe proposera une application du RGPD à travers les acteurs se trouvant autour du système blockchain (E).

A. Les blockchains publiques comme systèmes favorables à la protection de la vie privée

L'un des arguments en faveur de la Blockchain et l'une des raisons de son succès et développement (bien que, loin d'être l'unique raison) est qu'elle est supposée être favorable à la protection de la vie privée et la confidentialité de ses utilisateurs.[63] Ainsi, cette technologie propose une solution au problème de traitement massif des données fait par les entreprises et les autorités dans le monde traditionnel centralisé. Aucune autorité centrale ne contrôle le système ni ne stocke ou traite des données relatives à ses utilisateurs puisque le système est décentralisé et le registre des transactions est distribué à tous les nœuds du système qui n'ont en principe jamais eu besoin de révéler leur identité afin de se voir attribuer une paire de clefs – clef publique et clef privée.

Dans la plupart des blockchains publiques, les transactions sont pseudonymes : uniquement la clef publique des utilisateurs (qui n'est en aucun cas liée à l'identité de l'utilisateur puisqu'elle est délivrée de manière aléatoire par le système) est divulguée aux autres participants. Sur une blockchain, une transaction est faite grâce à l'utilisation de cette clef publique que l'on pourrait éventuellement considérer comme un pseudonyme, puis l'utilisateur se sert de sa clef privée et la combinaison des deux rend la transaction faisable. Ce système pourrait donc être comparé à un système de signature électronique : la combinaison de la clef publique et privée est nécessaire afin que l'utilisateur/l'utilisatrice puisse prouver son identité[64] et démontrer qu'il/elle est bien le/la propriétaire des montants transférés.

Les transactions s'effectuent de pair à pair et sont validées par certains nœuds du système qui effectuent une preuve de travail. Lorsqu'un nœud aura validé les transactions, elles pourront être inclues dans un nouveau bloc. De ce fait, l'on considère que le système est autonome et s'exécute par lui-même puisqu'il n'existe pas d'autorité centrale ou autre intermédiaire qui assure le fonctionnement du système ou vérifie la bonne volonté des parties à une transaction car le système lui-même et ses participants s'en chargent. Pour toutes ces raisons, les utilisateurs peuvent supposer qu'ils auront plus de confidentialité en utilisant des blockchains que d'autres types de services contrôlés par une autorité centrale.

63 Jordi Herrera-Joancomartì, Cristina Pérez-Solà, Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions. Torra V., Narukawa Y., Navarro-Arribas G., Yanez C. (eds) Modeling Decisions for Artificial Intelligence. MDAI 2016. Lecture Notes in Computer Science, vol. 9880. Springer, 2016, p. 14.

64 Anton Badev, Matthew Chen, Bitcoin: Technical Background and Data Analysis, Finance and Economics Discussion Series, Division of Research & Statistics and Monetary Affairs Federal Reserve Board, 2014-104, 7 octobre 2012, p. 8.

B. Le risque de déduction

Néanmoins, cela n'est pas si simple. Il faut rappeler qu'afin de créer une trustless trust (c'est à dire une confiance dans le système qui ne serait pas basée sur celle attribuée à une autorité centrale ou à un quelconque intermédiaire mais plutôt au système lui-même et à la preuve de travail mathématique), les blockchains publiques rendent disponible pour chaque participant au système le registre de toutes les transactions ayant déjà eu lieu de manière à ce que les différents nœuds du système puissent vérifier les transactions.

De ce fait, une blockchain est finalement bien plus transparente qu'un service ordinaire contrôlé par une autorité centrale. Cette transparence ne devrait théoriquement pas être problématique puisque les clefs publiques sont utilisées par les utilisateurs comme substituts à leur identité. Comme nous l'avons vu précédemment, les participants ne fournissent aucune information les concernant, pas même leur nom. Ils utilisent uniquement leur clef publique et leur clef privée de manière à ce que les transactions puissent s'effectuer et être enregistrées sur la blockchain.

Néanmoins, des recherches ont montré que les données que l'on peut trouver sur une blockchain, lorsqu'elles sont traitées avec les moyens technologiques adéquats, pourraient finalement être reliées à une personne physique.[65] Cela peut être fait par exemple en mettant en relation les données disponibles sur la blockchain et des données provenant d'en dehors du système ou encore en analysant le contexte d'une transaction sur une blockchain en faisant une analyse de réseau.[66] Il a déjà été prouvé qu'avec la connaissance technique adéquate, il est possible de déduire des relations entre différentes clefs publiques sur la blockchain Bitcoin. Dans certains cas, en utilisant des informations supplémentaires et disponibles en dehors du système, l'identité des utilisateurs peut aussi être déduite.[67] De plus, dans le cas de transactions à plusieurs entrées, une fois que le propriétaire d'une clef publique a été révélé, un lien peut être fait vers toutes les transactions relatives au même propriétaire.[68] Des chercheurs travaillent aussi afin de regrouper toutes les clefs publiques appartenant à un

65 Voir par exemple: Elli Androulaki, Ghassan Karame, Marc Roeschlin, Evaluating user privacy in Bitcoin, 2012 et Fergal Reid, Martin Harrigan, An analysis of anonymity in the Bitcoin System, Y/ Altshuler, Y. Elovici, A. Cremers, N. Aharony, A. Pentland, editors, Security and privacy in social networks, Springer, 2013.

66 Jordi Herrera-Joancomartì, Cristina Pérez-Solà, Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions. Torra V., Narukawa Y., Navarro-Arribas G., Yanez C. (eds) Modeling Decisions for Artificial Intelligence. MDAI 2016. Lecture Notes in Computer Science, vol. 9880. Springer, 2016, p. 14.

67 Fergal Reid, Martin Harrigan, An analysis of anonymity in the Bitcoin System, Y. Altshuler, Y. Elovici, A. Cremers, N. Aharony, A. Pentland, editors, Security and privacy in social networks, Springer, 2013, p. 203.

68 Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, p. 6.

même utilisateur.[69] Les systèmes décentralisés peuvent finalement être plus vulnérables en termes de protection des données que les services centralisés.[70]

L'on comprend donc que, même si les transactions sont pseudonymes et même si elles ne révèlent pas l'identité des utilisateurs, la protection des données sur une blockchain reste un enjeu majeur et les utilisateurs devraient être protégés contre les violations de leur droit fondamental à la protection des données, même lorsqu'ils utilisent ces types de nouvelles technologies. Même s'il est clairement dans l'intérêt des consommateurs de voir se développer l'utilisation de la technologie dans le secteur financier (de manière à ce qu'on leur propose des services plus efficaces et personnalisés) il faudrait aussi assurer que ces consommateurs reçoivent un niveau équivalent de protection des données.

C. Les risques pour la protection des données et le droit à une vie privée

Il est nécessaire de rappeler que la première utilisation qui a été faite de la technologie Blockchain a été la cryptomonnaie Bitcoin. Elle permet aux utilisateurs de s'adonner à des transactions financières en cryptomonnaie et donc leur donne la possibilité de se passer des services bancaires en se servant uniquement de la blockchain pour effectuer des transactions de pair à pair.

Les données bancaires et financières sont considérées par la jurisprudence de la Cour européenne des Droits de l'Homme (la « **CourEDH** ») comme des données personnelles et donc entrant dans le champ d'application de la CEDH, indépendamment du fait qu'il s'agisse d'informations sensibles ou non.[71] La consultation ou la saisie de données bancaires constitue une ingérence dans le droit de la personne concernée à une vie privée.[72] La CourEDH considère que les données bancaires incluent les relevés bancaires, les chèques ou encore les emails.[73]

Même si les transactions enregistrées sur une blockchain ne font pas partie de la liste que donne la CourEDH pour définir ce qui constitue des données bancaires et même si les transactions sur une blockchain sont la plupart du temps effectuées en cryptomonnaies et ne prévoient donc pas la participation d'une banque, les cryptomonnaies permettent malgré tout aux utilisateurs d'acheter ou de vendre des biens, ce qui constitue l'une des fonctions principales de la monnaie. Il pourrait être considéré que la consultation de données sur une blockchain peut fournir autant d'informations sur un individu que la saisie de ses documents bancaires permettrait. L'identité des utilisateurs devrait dès lors être protégée afin d'assurer le droit à la vie privée et le

69 Jordi Herrera-Joancomartì, Cristina Pérez-Solà, Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions. Torra V., Narukawa Y., Navarro-Arribas G., Yanez C. (eds) Modeling Decisions for Artificial Intelligence. MDAI 2016. Lecture Notes in Computer Science, vol. 9880. Springer, 2016, p. 14.

70 Primavera De Filippi, The interplay between decentralization and privacy: the case of blockchain technologies, Journal of peer production, 16 mai 2017, p. 1.

71 CourEDH, Brito Ferrinho Bexiga Villa-Nova c. Portugal, no. 69436/10, 1 décembre 2015, § 42.

72 *Idem*, § 44, CourEDH, M.N. et autres c. Saint-Marin, no. 28005/12, 7 juillet 2015, § 55.

73 CourEDH, M.N. et autres c. Saint-Marin, no. 28005/12, 7 juillet 2015, § 55.

droit à la protection des données des utilisateurs et cela pourrait être fait en appliquant les dispositions du RGPD aux blockchains.

D. Appliquer la définition de pseudonymisation prévue par le RGPD aux blockchains publiques

Néanmoins, l'application du RGPD aux blockchains pose certains problèmes. Le Parlement européen rappelle que la technologie Blockchain pose des questions spécifiques quant à l'utilisation des données de par son caractère décentralisé[74] qui seront analysées dans ce paragraphe. Premièrement, afin d'appliquer le RGPD à des blockchains, il faut se demander si les blockchains et les données traitées par le système entrent bien dans le champ d'application du RGPD. Le RGPD est applicable à de nombreux différents types de traitements de données personnelles et inclut la collecte, le stockage ou encore le fait de rendre disponible des données personnelles.[75] Puisqu'une blockchain distribue chacune des transaction ayant lieu aux différents nœuds du système en leur distribuant une copie de la blockchain (qui contient toutes les transactions ayant jamais eu lieu et les clefs publiques de chacune des parties à ces transactions), il paraît assez clair qu'une blockchain non seulement collecte et stocke des données relatives aux transactions et aux utilisateurs mais les rend aussi accessibles aux différents nœuds du système en distribuant une copie de la blockchain à chaque participant. L'utilisation des données faite dans le contexte d'une blockchain devrait donc être inclue dans la définition de traitement prévue par le RGPD.

Une autre question qui doit être résolue est celle de savoir si des données techniquement dites pseudonymes sur une blockchain pourraient aussi être considérées pseudonymisées juridiquement parlant.

D'après le RGPD, afin de déterminer si des données peuvent être attribuées à un individu identifié ou identifiable et donc si elles doivent être considérées comme personnelles (ou pseudonymisées) et non pas anonymes, l'on doit considérer tous les facteurs objectifs comme par exemple le coût et le temps nécessaire pour procéder à l'identification. Aussi, la technologie disponible au moment du traitement ainsi que les développements technologiques doivent être pris en considération.[76]

Les moyens techniques qui ont été mentionnés dans cet article et qui peuvent être utilisés afin de déduire des informations à partir d'une blockchain existent d'ores et déjà malgré le fait qu'ils soient particulièrement avancés. De plus en plus de start-ups proposant des services d'analyses de blockchains proposent leur assistance aux départements et services de business intelligence, de compliance ou encore aux autorités afin de déduire des données à partir d'une blockchain.[77]

---

74 Parlement européen, Commission des affaires économiques et monétaires, Rapport sur la technologie financière: influence de la technologie sur l'avenir du secteur financier, (2016/2243(INI)), 28 avril 2017, p. 18.

75 RGPD, art. 4(2).

76 RGPD, considérant 26.

77 Voir par exemple Chainanalysis, consulté le 30 octobre 2017, https://www.chainalysis.com/#about.

Pour cela, ces techniques qui permettent de déduire des informations à partir d'une blockchain devraient être prises en considération afin de décider si les données disponibles sur le système sont pseudonymes ou pas. De plus, puisqu'une confidentialité optimale n'est pas assurée, il serait sensé d'envisager que ce type de données devrait être considéré comme pseudonyme et non pas comme anonyme. Si tel est le cas, alors les données personnelles des utilisateurs sur une blockchain pourraient être protégées grâce à l'application des dispositions du RGPD.

Néanmoins, en examinant la définition de données pseudonymisées prévue par le RGPD, l'on peut voir que le législateur l'entend comme des « données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires » et qui, de ce fait, « devraient être considérées comme des informations concernant une personne physique identifiable. »[78] Les processus de pseudonymisation devraient donc permettre de retirer les identificateurs directs d'une donnée ou base de données afin de les remplacer par des pseudonymes. S'il n'y a pas de doute sur le fait que des données sur une blockchain pourraient être attribuées à une personne physique grâce à des informations supplémentaires, le premier critère que prévoit la définition pourrait être moins évident à prouver.

Comme nous l'avons vu précédemment, les informations contenues sur la plupart des blockchains publiques sont des données relatives à des clefs publiques, souvent désignées comme des pseudonymes[79] puisqu'elles sont utilisées comme substituts aux noms des utilisateurs. Une fois que la clef publique a été combinée à la clef privée correspondante, cela permet de signer la transaction. Aucun renseignement comme un nom ou autre information liée à la personne concernée n'a jamais été donné. Les identités réelles des utilisateurs n'ont donc pas été pseudonymisées et n'ont pas subi de processus de pseudonymisation : les identités réelles n'ont pas été changées puis remplacées par des clefs publiques pseudonymisées puisque les utilisateurs ne les ont jamais fournies. De ce fait, il n'est pas évident que les données sur une blockchain devraient être considérées comme entrant dans la définition des données pseudonymiséees que nous propose le RGPD.

Une interprétation possible du concept de pseudonymisation a été décrite par la doctrine juridique et considère que, aussi longtemps que la base de données non pseudonymisée n'a pas été détruite, alors la base de données transformée et pseudonymisée doit encore être considérée comme pseudonyme.[80] C'est uniquement lorsque la base de données initiale a été détruite que la base de données qui a été pseudonymisée peut être considérée comme anonyme et donc ne rentrant plus dans le champ d'application du RGPD. Si, en effet, cette manière d'envisager la pseudonymisation est exacte, alors les données sur une blockchain publique comme la blockchain Bitcoin pourraient ne pas être considérées comme pseudonymes mais comme anonymes puisqu'une base de données originale (et donc non pseudonymisée) n'existe pas

78 RGPD, considérant 26.

79 Primavera De Filippi, The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologiers, Journal of Peer Production, 16 mai 2017, p. 5.

80 Sophie Stalla-Bourdillon, Alison Knight, Anonymous data v. personal data – a false debate: an EU perspective on anonymisation, pseudonymisation and personal data, Southampton Law School, mars 2017.

et n'a donc pas pu être détruite. Nous sommes donc confrontés à la possibilité que, nonobstant les risques que rencontrent les utilisateurs de blockchains vis-à-vis de leur droit à la protection des données, il est probable qu'aucune règle en matière de protection des données ne leur soit applicable puisque la définition de pseudonymisation prévue par le RGPD ne prend pas en compte le phénomène de blockchains.

Plus de recherches devraient être menées quant à la possibilité de considérer que les données sur une blockchain publique puissent être inclues dans la définition de données personnelles plutôt que celle de données pseudonymes et de ce fait, entrer dans le champ d'application du RGPD.

E. Application via les acteurs se trouvant autour de la blockchain

Néanmoins, l'application de la définition de pseudonymisation pourrait être applicable aux blockchains si l'on se concentre sur les acteurs se trouvant autour de la blockchain et qui non seulement utilisent les informations disponibles sur la blockchain mais qui les mettent aussi en lien avec d'autres bases de données. Ces tierces parties ne sont pas seulement au courant des clefs publiques de leurs utilisateurs mais elles détiennent aussi des informations supplémentaires les concernant.

Même si les blockchains sont autonomes, fonctionnent par elles-mêmes et ne sont ni contrôlées par une autorité centrale ni ne nécessitent l'intervention d'un intermédiaire pour assurer leur fonctionnement, il existe bien des tierces parties. Elles permettent de rendre l'utilisation de blockchains plus facile, en particulier pour les non-techniciens. Elles permettent aussi de faire le lien entre, d'une part, les cryptomonnaies et, d'autre part, les monnaies ayant cours légal et l'économie traditionnelle. L'objectif de cette partie n'est pas de proposer une liste exhaustive des tierces parties existantes dans l'écosystème Blockchain. Cependant, les activités et le rôle de quelques-unes d'entre elles seront évalués et utilisés comme exemple.

Les fournisseurs de services de change de cryptomonnaies par exemple, d'une certaine façon, ont démocratisé l'utilisation de blockchains en permettant à quiconque d'acheter facilement de la cryptomonnaie à l'aide de monnaie ayant cours légal et sans avoir besoin d'investir dans des équipements particulièrement chers et performants afin de miner de la cryptomonnaie. Afin de proposer ce type de services, les fournisseurs de services de change de cryptomonnaies détiennent la plupart du temps les informations bancaires relatives à leurs consommateurs afin de reconnaître le transfert de monnaie ayant cours légal fait par le consommateur désireux de recevoir un montant équivalent de cryptomonnaie en échange. La plateforme d'échange Mt. Gox qui fût la plus importante sur le marché des cryptomonnaies, bien qu'elle se soit effondrée en 2014, avait pour habitude de demander une version scannée des papiers d'identité de ses consommateurs afin de leur permettre de déposer ou de retirer de la monnaie ayant cours légal.[81]

Les commerces acceptant d'être payés en cryptomonnaies doivent aussi être mentionnés. Puisqu'ils reçoivent un paiement, ils connaissent la clef publique de leurs con-

81 Malte Möser, Anonymity of Bitcoin Transactions, An Analysis of Mixing Services, Münster Bitcoin Conference, 17-18 juillet 2013.

sommateurs mais ils peuvent aussi détenir des informations supplémentaires. Par exemple, ils pourraient demander l'adresse email de l'utilisateur et ils pourraient aussi connaître l'adresse postale à laquelle le bien acheté grâce à de la cryptomonnaie devra être livré.

Finalement, le statut des blockchains privées est aussi à étudier. Leur fonctionnement est, technologiquement parlant, proche de celui des blockchains publiques mais une différence capitale est qu'il existe une autorité centrale qui exerce son contrôle quant aux personnes ayant un droit de participation. Tout le monde ne peut pas participer à la blockchain puisqu'il faut auparavant avoir obtenu un droit d'accès.[82] Ainsi, l'autorité connaît l'identité des consommateurs et ce type de blockchain peut finir par être entièrement centralisé autour d'une autorité.[83]

Ces trois acteurs qui peuvent connaître l'identité de leurs utilisateurs, pourraient ainsi éventuellement être en mesure de relier une identité digitale (une clef publique) avec l'identité réelle des utilisateurs et ainsi retracer toutes les transactions exécutées les concernant.[84]

Revenons à l'interprétation qui considère la définition de pseudonymisation proposée par le RGPD comme un moyen de supposer que des données pseudonymisées entrent dans le champ d'application du RGPD jusqu'à ce que la base de données non pseudonymisée ait été détruite : alors ces trois acteurs devraient être considérés comme des responsables de traitement ou des sous-traitants et donc être soumis aux obligations prévues par le RGPD.

Finalement, l'on comprend que même si le droit à la protection des données des utilisateurs de blockchains peut être mis en danger par de nouveaux moyens technologiques, l'application du RGPD aux services développés sur une blockchain soulève un certain nombre d'interrogations, comme nous l'avons vu précédemment. Une possibilité pour permettre l'application du RGPD pourrait être de se concentrer sur les acteurs autour de la blockchain et qui font le lien entre le monde digital d'une part et le monde réel d'autre part.

IV. Le manque de sécurité juridique et ses conséquences sur le niveau de protection des droits fondamentaux

Nous avons vu en introduction que le RGPD assure la protection des données de deux manières différentes : comme moyen de régulation des risques reposant sur les responsables du traitement et les sous-traitants et comme moyen de contrôle individuel reposant sur les personnes concernées. Les incertitudes qui ont été examinées dans cet article prouvent que, pour le moment, de nombreuses interrogations doivent encore être examinées. En ce qui concerne le droit fondamental à la protection des données des utilisateurs de blockchains: la sécurité juridique n'est pas pleinement assurée à

82 Patrick Waelbroeck, Les enjeux économiques de la blockchain, Annales des Mines – Réalités industrielles 2017/3, août 2017, p. 10.

83 *Idem*, p. 13.

84 Rainer Böhme, Nicolas Christin, Benjamen Edelman, Tyler Moore, Bitcoin: Economics, Technology, and Governance, Journal of Economic Perspectives, vol. 29, no. 2, printemps 2015, p. 221.

l'heure d'aujourd'hui. C'est pourquoi, l'on pourrait argumenter que la protection des données comme moyen de régulation des risques ne sera pas suffisante comme moyen de protéger les données des utilisateurs si ces incertitudes ne sont pas réglées. Ces incertitudes pourraient donc conduire au besoin pour les utilisateurs d'être plus impliqués dans la protection de leurs données et leur intervention pourrait donc aller au-delà du simple exercice de leurs droits qui découlent des mesures de contrôle individuel que l'on retrouve dans les dispositions du RGPD. Dans cette dernière partie, il s'agira de démontrer que les incertitudes décrites ci-dessus pourraient provoquer un mouvement d'une approche individualiste équilibrée à une approche individualiste stricte de la protection des données (A). Une conséquence pourrait être que la connaissance technologique finisse par devenir une condition préalable à une protection des données adéquate (B).

A. Protection des données : d'une approche individualiste équilibrée à une approche individualiste stricte

Premièrement les personnes concernées peuvent décider d'exercer les différents droits qu'ils retirent des dispositions du RGPD. Ils peuvent par exemple décider d'utiliser leur droit d'accès aux données, leur droit de rectification ou leur droit à l'oubli. Ensuite, ils peuvent aussi décider d'utiliser des services supplémentaires ou de s'adonner à des pratiques additionnelles et visant à procurer plus de sécurité et de confidentialité lorsqu'ils utilisent des blockchains. Les individus peuvent décider aussi d'utiliser eux-mêmes des techniques afin d'assurer la confidentialité (techniques qui sont par ailleurs encouragées par le RGPD) comme le cryptage de leurs transactions.

Ce phénomène est déjà en train de se produire dans le domaine des blockchains. Premièrement, au sein de la communauté blockchain, il est largement encouragé de mettre en place des techniques de confidentialité assez simples comme la génération d'une paire de clefs supplémentaire pour chaque nouvelle transaction qui est faite.[85] Il est aussi conseillé à l'utilisateur de s'envoyer à lui-même et de manière répétée des fractions du montant de cryptomonnaie détenu mais en utilisant une nouvelle clef publique à chaque fois.[86] Aussi, des entreprises et start-ups ont développé des services permettant plus de confidentialité pour les transactions sur les blockchains. Certains services proposent par exemple de rendre invisible le contenu des transactions alors que d'autres proposent aussi de rendre invisibles les métadonnées associées à ces transactions.[87]

Un autre mécanisme visant à permettre plus de confidentialité est particulièrement développé et encouragé dans l'écosystème Blockchain : il s'agit de l'utilisation de mixeurs afin de permettre plus de confidentialité à l'identité des parties à une transaction. Les mixeurs permettent d'augmenter la confidentialité en mélangeant des unités

85 Primavera De Filippi, The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies, Journal of Peer Production, 16 mai 2017, p. 6.

86 Fergal Reid, Martin Harrigan, An analysis of anonymity in the Bitcoin System, Y. Altshuler, Y. Elovici, A. Cremers, N. Aharony, A. Pentland, editors, Security and privacy in social networks, Springer, 2013, p. 203.

87 Voir par exemple Zerocash, consulté le 30 octobre 2017, http://zerocash-project.org.

de cryptomonnaie de multiples utilisateurs et donc en rendant plus difficile la mise en relation des entrées et sorties de transactions sur une blockchain. Leur fonctionnement est le suivant : l'initiateur d'une transaction fait une transaction vers une clef publique appartenant au mixeur. Plus tard, le mixeur transfère un montant équivalent au destinataire mais en utilisant une clef publique différente de celle sur laquelle il avait reçu la transaction de l'initiateur. Dès lors, le destinataire de la transaction recevra bien le montant de la transaction mais celui-ci ne sera plus relié à l'initiateur de la transaction. Par conséquence, le lien entre les participants à une transaction sera plus difficile à établir et plus de confidentialité sera assurée aux participants.[88]

B. La connaissance technologique comme condition préalable à un niveau adéquat de protection des données

Cependant, le fait de donner aux individus une possibilité de contrôle sur les données les concernant (soit en exerçant les droits qui découlent du RGPD soit en introduisant d'autres techniques ayant pour but d'assurer la confidentialité) peut être risqué en termes de protection des données et donc de droits fondamentaux. En effet, si l'on considère que la protection des données est uniquement un moyen de contrôle individuel, le niveau de protection des données que reçoivent les personnes concernées dépendra de leur engagement et de leur niveau d'attention quant à la protection de leurs données. Pour bénéficier d'un niveau adéquat de protection des données les personnes concernées devraient premièrement être conscientes des enjeux relatifs et des droits qu'ils retirent des dispositions du RGPD de manière à pouvoir les exercer. Deuxièmement, elles devraient avoir une compréhension suffisante de la technologie qui leur permettrait de mettre en place des techniques supplémentaires afin d'assurer leur confidentialité.

De plus, il est important de noter que le traitement des données devient de nos jours très complexe et de ce fait, particulièrement difficile à comprendre pour des personnes qui ne sont pas expertes en technologie.[89] Les personnes concernées ne devraient pourtant pas avoir besoin d'être des experts en confidentialité pour recevoir un niveau adéquat de protection des données.[90] Dès lors, les individus devraient plutôt partager le contrôle sur leurs données personnelles plutôt que l'exercer seuls afin que l'ensemble des personnes concernées puisse bénéficier d'un niveau de protection adéquat.

En effet, le mouvement que l'on a analysé d'une approche individualiste équilibrée à une approche individualiste stricte en termes de protection des données est contraire au souhait du législateur européen. Il faut rappeler que le RGPD vise, entre autre, à mettre en place des mesures de protection des données dès la conception et par défaut de manière à ce que, par défaut, les personnes concernées puissent bénéficier d'un ni-

88 Malte Möser, Anonymity of Bitcoin Transactions, An Analysis of Mixing Services, Münster Bitcoin Conference, 17-18 juillet 2013.

89 Prof. Lokke Moerel, Prof. Corien Prins, Privacy for the *homo digitalis*, Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things, Tilburg Institute for Law, Technology, and Society, 2016, p. 62.

90 Daniel Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. Law Rev. 1880, 2013, p. 1901.

veau adéquat de protection des données. Le traitement des données devrait alors respecter le droit des individus à la protection des données, et ce même s'ils ne s'engagent pas personnellement dans la protection de leurs données personnelles. Des auteurs considèrent qu'un droit à l'ignorance devrait exister comme droit à part entière et faisant partie des droits fondamentaux.[91] L'idée derrière cela est que l'ignorance d'un individu, ou en l'espèce son manque de connaissance technique, ne devrait pas résulter en un affaiblissement de la protection de ses droits fondamentaux. Il semblerait que ce point de vue soit partagé au niveau de l'Union européenne. En effet, même si les institutions européennes encouragent le contrôle individuel sur les données personnelles,[92] il est clair que pour le législateur européen, ces mesures de contrôle individuel ne doivent exister qu'à côté d'un environnement favorable à la protection des données et en supplément de mesures adéquates dont les personnes concernées peuvent bénéficier.[93] Ainsi, la protection des données personnelles ne peut pas être entièrement assurée par les individus eux-mêmes s'ils ne sont pas soutenus par des mesures imposées aux responsables du traitement et sous-traitants. La protection des données basée sur des mesures de contrôle individuel uniquement risque de mener à des niveaux différents de protection des données et donc à une nouvelle hiérarchie au sein de laquelle les spécialistes en technologie bénéficieraient d'un niveau de protection adéquat de leur droit fondamental à la protection des données grâce à l'utilisation de services supplémentaires lorsque d'autres n'en bénéficieront pas. Malheureusement, un niveau adéquat de protection des données personnelles ne devrait pas être sujet à des connaissances techniques ou technologiques.

Finalement, ce double niveau de protection des données qui résulte des incertitudes relatives à l'application du RGPD aux FinTech est contreproductif pour le développement de l'innovation et de la technologie. Au contraire, un niveau élevé de protection des droits fondamentaux des utilisateurs servirait l'amélioration et le développement des FinTech puisqu'il permettrait d'améliorer l'image que ces services donnent aux consommateurs potentiels et à la société dans son ensemble.

Conclusion

Le traité de Lisbonne a indiqué le souhait de promouvoir le développement de la protection des droits fondamentaux au sein de l'Union européenne à travers la création d'un espace de liberté, de sécurité et de justice. De plus, le respect des droits fondamentaux est d'une importance capitale puisqu'il s'agit de l'une des valeurs sur lesquelles s'est construite l'Union européenne et qui est aussi étroitement liée à la notion

91 Voir Prof. Lokke Moerel, Prof. Corien Prins, Privacy for the *homo digitalis*, Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things, Tilburg Institute for Law, Technology, and Society, 2016, p. 84 et la référence faite à Arnon Grunberg qui plaide pour l'introduction d'un droit à l'ignorance comme droit fondamental, Arnon Grunberg, 2015, p. 15.

92 Voir par exemple Commission européenne, Direction générale de la justice, Prends le contrôle de tes données personnelles, 2012.

93 Christophe Lazaro, Daniel Le Métayer, The control over personal data: True remedy or fairy tale?, Project-Teams Privatics, Research Report no. 881, 13 avril 2015, p. 21.

de l'Etat de droit. La protection des données personnelles comme partie intégrante des droits fondamentaux au sein de l'Union européenne est assurée par la Charte des droits fondamentaux de l'Union européenne et par le TFUE.

Les développements technologiques ont provoqué le besoin de mettre en place un niveau élevé de protection des données au sein de l'Union européenne qui répondrait aux enjeux soulevés par le développement technologique et qui n'étaient pas traités par la Directive 95/46 qui a été publiée en 1995, c'est-à-dire bien avant l'époque du Big data et l'utilisation massive de la technologie dans divers secteurs de notre société. C'est pourquoi le RGPD est supposé être plus adapté aux enjeux récents. Il n'impose pas seulement des mesures de protection des données aux responsables de traitement et sous-traitants mais il donne aussi des droits individuels aux personnes concernées : il comprend des mesures de régulation des risques et des mesures de contrôle individuel et de ce fait, il est supposé assurer un haut niveau de protection des données à toutes les personnes concernées indépendamment du fait qu'elles utilisent des services supplémentaires promettant plus de confidentialité.

Cependant, les récents développements du secteur financier ne sont pas nommés par le RGPD. Il n'est pas fait référence aux FinTech et à la manière dont leurs différences avec les acteurs financiers traditionnels doivent être abordées afin d'assurer aux consommateurs un niveau équivalent de protection des données. Les FinTech sont une grande opportunité pour le secteur bancaire et financier mais aussi pour les consommateurs parce qu'ils leur permettent de se voir proposer des services plus personnalisés, plus transparents et moins coûteux. Néanmoins, afin de rester dans l'intérêt des utilisateurs, ils ne devraient pas mettre en danger la confidentialité et les droits fondamentaux des utilisateurs.

Cet article vise à mettre en lumière certaines interrogations qui devraient être traitées par le législateur ou par la jurisprudence de manière à ce que les consommateurs puissent finalement bénéficier, quand ils utilisent des FinTech, d'un niveau adéquat et équivalent de protection des données.

Premièrement, il faudrait clarifier qui doit être considéré comme responsable du traitement ou sous-traitant et donc qui est soumis aux obligations prévues par le RGPD. La particularité des services de cloud computing a été mise en évidence dans cet article et permet d'attirer l'attention sur la possibilité qu'ils se voient sanctionner alors qu'ils n'étaient pas même conscients des activités auxquelles se livraient leurs clients. C'est pourquoi il faudrait clarifier la question de savoir si les règles d'exonération de responsabilité qui sont prévues par la Directive sur le commerce électronique (qui, pour le moment, exclut les questions de protection des données de son champ d'application) s'appliquent aux intermédiaires dans le cas de traitement de données. Aussi, il est nécessaire de déterminer qui doit être considéré comme responsable du traitement ou sous-traitant sur une blockchain publique.

Deuxièmement, des interrogations par rapport à la qualification et la définition des données personnelles, anonymes et pseudonymisées doivent être traitées. La qualification de données comme anonymes devrait prendre en considération le risque de réidentification qui est sans cesse présent au vu du développement infini de la technologie. Une possibilité pourrait être d'introduire une évaluation des risques régulière de manière à ce que le processus d'anonymisation puisse être testé par rapport aux moyens technologiques disponibles, au traitement fait à partir des données ainsi que par

rapport aux possibles mises en relation avec d'autres bases de données. Aussi, puisque la qualification de données comme pseudonymisées ne permet pas aux responsables du traitement d'obtenir des règles plus souples, les codes de conduite ou les mécanismes de certification devraient être pris en compte lorsqu'une violation se produit, afin de prouver le souhait de se mettre en conformité avec le RGPD. Ainsi, cela constituerait une forte incitation pour les responsables du traitement à mettre en place des techniques de pseudonymisation.

Troisièmement, des instructions sont nécessaires quant à l'application du RGPD qui devrait être faite aux blockchains. Même si les données disponibles sur une blockchain sont souvent décrites comme pseudonymes, elles ne remplissent pas entièrement la définition prévue par le RGPD. En effet, les données sur une blockchain n'ont jamais subi de processus de pseudonymisation puisqu'elles n'ont jamais été reliées à l'identité des personnes concernées. Cela n'empêche pas les techniciens et les scientifiques d'être capables d'identifier des utilisateurs à partir de leur clef publique, en utilisant les informations disponibles sur la blockchain et en dehors. Ainsi, si les données sur une blockchain ne peuvent pas être considérées comme pseudonymisées d'après la définition prévue par le RGPD, il existe un risque que les données des utilisateurs ne soient finalement pas protégées. Cela pourrait avoir des conséquences majeures puisque la divulgation d'une identité relative à une clef publique peut mener à la possible déduction de toutes les transactions ayant jamais été faites et auxquelles cette clef publique a participé. Cela pourrait avoir des conséquences sévères sur la vie privée de la personne concernée. Le rôle des tierces parties qui évoluent autour de la blockchain doit aussi être abordé puisque, la plupart du temps, elles détiennent des informations supplémentaires relatives à leurs consommateurs qui pourraient permettre de les identifier assez facilement. Le rôle des blockchains privées doit aussi être pris en compte.

Les incertitudes juridiques qui ont été traitées dans cet article ont des conséquences négatives sur le droit à la protection des données des utilisateurs. Puisque la manière dont le RGPD doit s'appliquer aux FinTech n'est pas encore clairement définie; jusqu'à ce que ces questions soient résolues, les mesures de régulation des risques imposées sur les responsables du traitement et les sous-traitants pourraient ne pas être réellement efficaces dans le cas des FinTech. Ainsi, les utilisateurs de blockchains peuvent décider d'agir par eux-mêmes. Premièrement, ils peuvent décider d'exercer les mesures de contrôle individuel prévues par le RGPD. Cela peut aussi s'avérer compliqué à cause des incertitudes mentionnées précédemment. Ils peuvent alors décider de mettre en place leurs propres pratiques et d'utiliser des techniques promettant plus de confidentialité. Cela est d'ores et déjà encouragé dans l'écosystème Blockchain au sein duquel les utilisateurs sont incités à générer une nouvelle paire de clefs pour chaque nouvelle transaction qu'ils réalisent. Ils peuvent aussi décider d'utiliser des nouveaux services, comme les mixeurs, qui leur proposent une meilleure protection de leur identité.

Ce mouvement dans la manière dont est envisagée et assurée la protection des données peut avoir des conséquences négatives pour les utilisateurs. L'on peut craindre que les connaissances techniques et technologiques deviennent des conditions *sine qua non* d'un niveau adéquat de confidentialité et passant par l'utilisation de techniques additionnelles. Dès lors, le niveau de protection des données pour les utilisateurs

de FinTech dépendra du niveau de conscience de la personne concernée quant aux enjeux de la protection des données et du niveau de son engagement pour l'assurer. Finalement, le risque pourrait être que les connaissances techniques deviennent la condition préalable à une protection des données efficace. Dans ce cas, un niveau adéquat de protection des droits fondamentaux ne sera plus assuré à toutes les personnes concernées par les traitements de données.

C'est pourquoi, un premier pas pour faire face à ces difficultés sera d'assurer un niveau adéquat de protection des données par défaut aux personnes concernées. Ainsi, les responsables du traitement et sous-traitants devraient être conscients de la manière dont ils doivent mettre en place les mesures de régulation des risques prévues par le RGPD. Concernant les FinTech, cela sera possible uniquement lorsque certaines interrogations (y compris celles mentionnées dans cet article) seront traitées et clarifiées et donc lorsque la sécurité juridique sera assurée.