# Y a-t-il un pilote dans la blockchain ? Réflexions sur l'identification d'un responsable de traitement dans le cadre de la blockchain

Alice Mornet

# Y a-t-il un pilote dans la *blockchain* ?
## Réflexions sur l'identification d'un responsable de traitement dans le cadre de la *blockchain*

**Alice MORNET**

Vouée à devenir le « nouveau moteur de l'économie mondiale »[1], la *blockchain* est l'objet de nombreux fantasmes. Qualifiée de disruptive ou de révolutionnaire, elle se révèle évanescente et demeure difficilement saisissable pour les non-initiés. Sa définition est pourtant aisée : la *blockchain* est une technologie de stockage et de transmission d'informations[2]. Elle apparaît, concrètement, comme une grande base de données contenant l'historique de l'ensemble des opérations réalisées depuis sa création. Utilisant des procédés relativement anciens — réseaux pair-à-pair ; cryptographie asymétrique — elle se singularise par ses caractéristiques. Transparence, sécurité et désintermédiation constituent ainsi le triptyque donnant à la technologie *blockchain* toute sa valeur. Élaborée dès 2008 avec le « *bitcoin* », elle connaît aujourd'hui de nouveaux usages et promet de s'étendre à d'autres domaines[3]. Profondément inédite, la *blockchain* se développe en niant les règles de protection des données à caractère personnel[4] qui connaissent, elles aussi, une évolution fulgurante. Trouvant leur origine dans la loi Informatique et Libertés du 6 janvier 1978, elles ont été sensiblement remaniées par le règlement (UE) 2016/679 (ci-après « RGPD »)[5].

Opposer les règles du RGPD à la *blockchain* n'a de sens que si celle-ci contient effectivement des données à caractère personnel[6]. Sur ce point, il existe aujourd'hui un

[1] G. MAZZOLINI, « La blockchain, nouveau moteur de l'économie mondiale », Les Échos, 7 déc. 2020.
[2] L'ordonnance n°2016-520 du 28 avril 2016 a introduit une définition de la *blockchain* au sein de l'article L.223-12 du Code monétaire et financier aux termes duquel celle-ci est définie comme « un dispositif d'enregistrement électronique partagé permettant l'authentification » des opérations réalisées.
[3] Sur les différentes utilisations de la *blockchain* : M. MEKKI, « Les mystères de la blockchain », Rec. D., 2017, p. 2160.
[4] La technologie fragilise de nombreuses dimensions du droit à la protection des données. Par exemple, son immuabilité interdit, en principe, toute rectification ou suppression de données. De même, sa distribution internationale empêche de déterminer, précisément, le droit applicable. V. not. au sujet de ces difficultés, J. DEROULEZ, « L'actualisation des enjeux liés aux données personnelles. Blockchain », Lamy Droit de l'Immatériel, n°156, 2019 ; F. CHAFIOL, A. BARBET-MASSIN, « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », Dalloz IP/IT, 2017, p. 637 ; T. DOUVILLE, « Blockchain et protection des données à caractère personnel », AJ Contrat, 2019, p. 316.
[5] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4 mai 2016, p. 1.
[6] Le RGPD subordonne son application à la présence d'un traitement de données à caractère personnel : Art. 1§1, *Ibid*.

consensus[7] et d'aucuns contestent la présence de telles données sur la *blockchain* et, *de facto*, l'application du RGPD. Technologiquement réalisable[8], un anonymat total[9] l'écarterait mais serait alors susceptible de nuire à la prévention et à la lutte contre la criminalité[10]. La *blockchain* doit donc se soumettre au RGPD et cette conciliation constitue, selon le Professeur Mekki, « l'enjeu de demain »[11].

Entré en vigueur en 2016, le RGPD a pour ambition d'« instaurer un cadre solide, cohérent et moderne » en matière de protection des données « qui soit neutre sur le plan technologique et résistant à l'épreuve du temps pour plusieurs décennies »[12]. Le principe de neutralité dont le RGPD se prévaut implique alors qu'il puisse résister aux évolutions technologiques[13]. Pourtant, nombreux sont les auteurs ayant souligné son apparente incompatibilité avec la *blockchain*[14]. Si plusieurs points d'achoppement ont été relevés, l'identification d'un responsable de traitement interroge particulièrement. Obéissant à une analyse contextuelle et factuelle[15], la détermination de ce personnage central suppose d'identifier la partie définissant la finalité — le but — et les moyens du traitement — le comment[16]. Si elle apparaît parfois évidente, cette identification peut également se révéler

[7] F. CHAFIOL, A. BARBET-MASSIN, « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », *op. cit.* ; M. POPPE, « Quelle relation entre la protection des données à caractère personnel et la blockchain ? », Revue Lamy droit des affaires, n°129, 2017 ; O. LASMOLES, « La difficile appréhension des blockchains par le droit », Revue internationale de droit économique, 2018/4, t. XXXII, pp. 453-469 ; CNIL, *Blockchain : Premiers éléments d'analyse de la CNIL*, Sept. 2018, 11 p. ; S. CULLAFFROZ-JOVER, E. BACQ, « Blockchain et données à caractère personnel, l'improbable conciliation ? », Droit et Patrimoine, n°290, 2019.

[8] Le procédé cryptographique dit de « la preuve sans divulgation de connaissance » semble susceptible d'assurer un certain anonymat : V. FAURE-MUNTIAN, C. de GANAY, R. LE GLEUT, Rapport sur les enjeux technologiques des blockchains (chaînes de blocs), Sénat, 20 juin 2018 ; T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *op. cit*.

[9] Les données présentes sur la *blockchain* sont cryptées et n'apparaissent pas en clair. Toutefois, elles ne sont pas anonymes mais simplement « pseudonymisées », au sens du RGPD, en ce que l'identification de la personne concernée demeure permise. V. à ce sujet, J. DEROULEZ, « L'actualisation des enjeux liés aux données personnelles. Blockchain », *op. cit*.

[10] A. ELKAHWAGY, « La délinquance économique à l'heure du numérique : *Bitcoin*, blanchiment et autres observations », Arch. pol. crim., n°39, 2017, pp. 55-66.

[11] M. MEKKI, « Le smart contract, objet du droit (Partie 2) », Dalloz IP/IT, 2019, p. 27.

[12] Proposition de 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 (règlement général sur la protection des données), COM(2012) 11 final, p. 115.

[13] À propos de ce principe : A. ROBIN, « Neutralité du Net : vers une consécration européenne du principe ? », Comm. com. électr., 2015, étude 12.

[14] J. DEROULEZ, « Blockchain et données personnelles. Quelle protection de la vie privée ? », JCP G, n°38, 2017, 973 ; F. CHAFIOL, A. BARBET-MASSIN, « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », *op. cit.* ; M. POPPE, « Quelle relation entre la protection des données à caractère personnel et la blockchain ? », *op. cit.* ; T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *op. cit*.

[15] G29, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »,* WP 169, 16 fév. 2010, p. 9 ; EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2 sept. 2020, p. 10.

[16] G29, *Avis 1/2010, op. cit*., p. 14 ; EDPB, *Guidelines 07/2020*, *op. cit*., p. 13.

extrêmement complexe[17]. Fonctionnelle, la notion de responsable de traitement permet d'attribuer les responsabilités[18] et, ainsi, de garantir l'effectivité des dispositions du RGPD[19]. Or, dans les méandres de la *blockchain*, cette qualité peine à trouver son sujet et fragilise alors le droit à la protection des données à caractère personnel.

Si l'identification d'un responsable de traitement au sens du RGPD semble impossible dans le cadre de la blockchain (**I**), une responsabilisation de ses acteurs, à l'aune du droit de la responsabilité civile, paraît permise (**II**).

## I. Les limites rédhibitoires du RGPD : l'impossible identification d'un responsable de traitement dans la *blockchain*

Nombreux sont les auteurs à dénoncer la difficulté[20], voire l'impossibilité[21], qu'il y a à identifier les responsables de traitement dans le cadre d'une *blockchain*. Une telle gêne, résultant de l'incompatibilité structurelle existante entre la blockchain et le RGPD (**A**) empêche, il est vrai, d'identifier précisément un responsable de traitement (**B**).

### A. Une impossibilité résultant d'une incompatibilité structurelle

Alors que le RGPD devrait présenter une certaine neutralité technologique, sa logique semble incompatible avec celle de la *blockchain*[22].

Dans sa conception originelle, la technologie *blockchain* apparaît horizontale. Toutefois, il convient d'opérer une distinction selon que celle-ci est privée, par *consortium* ou

[17] EDPB, *Guidelines 07/2020*, *op. cit*., p. 11 et 15.
[18] G29, *Avis 1/2010*, *op. cit*., p. 10 ; EDPB, *Guidelines 07/2020, op. cit.*, p. 3.
[19] G29, *Avis 1/2010 op. cit*., p. 7.
[20] E. A. CAPRIOLI, « Les enjeux juridiques et sécurité des blockchains », Cahiers de droit de l'entreprise, n°3, 2017, dossier 19 ; Simmons & Simmons LLP, « Le droit et la technologie blockchain : une approche sectorielle », Contrats Concurrence Consommation, n°10, 2017, étude 10 ; O. LASMOLES, « La difficile appréhension des blockchains par le droit », *op. cit*., pp. 453-469 ; T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *op. cit*.
[21] L.-D. IBANEZ, K. O'HARA, E. SIMPERL, "On Blockchains and the General Data Protection Regulation", EU Blockchain Forum and Observatory, 6 July 2018, p. 10 ; J. DEROULEZ, « Quel responsable de traitement ? », Revue Lamy Droit de l'Immatériel, n°156, 2019.
[22] V. également en ce sens, T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *op. cit*.

publique[23]. Alors que les deux premières catégories admettent une certaine hiérarchie[24], la troisième est la seule à réunir les qualités d'une véritable *blockchain*. Caractérisée par l'horizontalité, la décentralisation et la distribution, ses intervenants sont strictement égaux et n'ont, *a priori*, aucune obligation les uns envers les autres. En outre, aucun tiers de confiance n'est chargé de veiller à la conformité de la chaîne, cette fonction étant dévolue à l'ensemble des membres participants. Plusieurs acteurs coexistent, en effet, dans le cadre d'une *blockchain*. Les développeurs et programmeurs sont les premiers intervenants en ce qu'ils déterminent son architecture et son fonctionnement. Les utilisateurs, quant à eux, écrivent sur la chaîne et l'utilisent pour réaliser une transaction ou pour enregistrer une information. Les mineurs en constituent le maillon indispensable en étant chargés de vérifier les transactions qui s'y opèrent. Les nœuds, enfin, détiennent le registre, doivent valider les transactions opérées sur la *blockchain* et peuvent, sous réserve d'atteindre un consensus suffisant, en modifier les règles. Si la présentation ne peut qu'être synthétique, il convient de préciser qu'aucune de ces qualités n'est exclusive et qu'il est tout à fait possible, par exemple, de cumuler le rôle de participant et de mineur, comme il est obligatoire, pour être mineur, d'être également un nœud du réseau. Ce *quatuor* d'acteurs, indispensable au bon fonctionnement d'une *blockchain*, accueille parfois d'autres intervenants. Il en va ainsi des oracles et des plateformes intermédiaires. Tandis que les premiers assurent l'exécution des *smart contracts* éventuellement intégrés dans la chaîne[25], les secondes sont chargées de vendre ou d'échanger les *bitcoins* ou autres cryptomonnaies nécessaires à son utilisation.

Le régime de protection des données répond, quant à lui, à un modèle vertical et centralisé. Conformément à son caractère fondamental[26], le droit à la protection des données suppose que la personne dont les données sont traitées — la « personne concernée » — dispose

[23] Pour une présentation des différents types de blockchain : M. MEKKI, « *If code is law, then code is justice ?* Droits et algorithmes », Gaz. Pal., n°24, 2017, p. 10 ; M. MEKKI, « Les mystères de la blockchain », *op. cit*., p. 2160.

[24] Dans une blockchain privée, une autorité centrale est chargée de maitriser la chaîne et les relations peuvent être contractualisées. De même, pour les blockchains par *consortium*, les participants sont limitativement énumérés et des responsables peuvent être érigés par contrat : D. LEGEAIS, « Blockchain » *in J-Class. Banque – Crédit – Bourse, Fasc. 179*, 1er janv. 2020, n°12.

[25] Les smart contracts sont des programmes informatiques pouvant exécuter automatiquement certaines instructions préalablement définies. Quant aux oracles, ils permettent d'intégrer à la *blockchain* des variables issues du monde réel. Sur ces notions : C. ZOLYNSKI, « Blockchain et smart contracts : premiers regards sur une technologie disruptive », Revue de droit bancaire et financier, janvier-février 2017, doss. 4 ; M. MEKKI, « Le contrat, objet des smart contracts (Partie I), Dalloz IP/IT, 2018, p. 409 ; M. MEKKI, « Le smart contract, objet du droit (Partie 2) », *op. cit*., p. 27.

[26] V. not. à ce sujet, E. DEBAETS, *Le droit à la protection des données personnelles : recherche sur un droit fondamental*, thèse dactylographiée, Paris 1, 2014, 811 p.

de prérogatives propres à garantir leur sauvegarde. Pour exercer ses droits[27], elle doit s'adresser aux « responsables de traitement », c'est-à-dire aux personnes physiques ou morales qui définissent les moyens et les finalités du traitement[28]. Tenus de répondre aux sollicitations des personnes concernées, ces derniers sont également chargés de veiller à la sécurité du traitement et, plus largement, au respect des exigences du RGPD[29]. À ce duo d'acteurs s'ajoutent parfois des « sous-traitants » qui recouvrent les personnes physiques ou morales traitant les données pour le compte du responsable de traitement[30]. Déterminantes, ces qualités commandent le bénéfice de droits ou l'attribution d'obligations en organisant, *de facto*, la protection des données à caractère personnel. S'articulant autour du responsable de traitement, le régime imposé se révèle profondément vertical et le RGPD a encore accentué ce trait distinctif en densifiant le rôle de cet acteur qui doit désormais veiller, de manière autonome, à la conformité de ses opérations[31].

L'identification d'un responsable de traitement apparaît indispensable à l'effectivité du droit à la protection des données à caractère personnel. Pourtant, la *blockchain*, de par ses multiples intervenants et sa structure décentralisée, semble résister à cette condition *sine qua non*.

### B. Une impossibilité apparemment irréversible

Fondamentale, la question de l'identification du responsable de traitement au sein de la *blockchain* n'est pas totalement éludée par la doctrine. Néanmoins, au regard des spécificités de la technologie, des divergences d'appréciation subsistent et, faute de consensus, aucune figure ne semble se démarquer.

Pour certains auteurs, les plateformes d'échange de jetons méritent d'être qualifiées de responsables de traitement[32]. S'il est vrai qu'elles collectent les données des utilisateurs tout en définissant les finalités et les moyens d'un tel traitement, elles n'interviennent pas dans le

[27] Sur les droits dévolus aux personnes concernées et leurs modalités d'exercice : Chapitre III, Règlement (UE) 2016/679, précité.
[28] Art. 4§7, *Ibid*.
[29] Sur les obligations imposées aux responsables de traitement : Chapitre IV, *Ibid*.
[30] Art. 4§8, *Ibid*.
[31] Conformément au principe d'*accountability* : A. DEBET, « Les nouveaux instruments de conformité », Dalloz IP/IT, 2016, p. 592 ; N. METALLINOS, « Le principe d'*accountability* : des formalités préalables aux études d'impact sur la vie privée (EIVP) », Comm. com. électr., n°4, 2018, étude 11.
[32] F. CHAFIOL, A. BARBET-MASSIN, « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », *op. cit*., p. 637.

fonctionnement concret de la *blockchain*[33]. D'autres auteurs attribuent la qualité de responsable de traitement aux concepteurs[34]. Incontestablement, ce sont eux qui conçoivent l'architecture de la chaîne. Cependant, la finalité déterminée reste à ce stade très large, une *blockchain* n'étant qu'un protocole pouvant servir de nombreux usages. Par exemple, *Ethereum* permet de développer une multitude d'applications parmi lesquelles la vente d'actifs ou la location de stockage *cloud*. La responsabilité pourrait alors être recherchée sur les concepteurs de ces applications, déterminant plus finement la finalité du traitement. Néanmoins, si cela autorise l'utilisateur, en tant que personne concernée, à contacter ces derniers afin d'exercer ses droits, une faille de sécurité imputable à *blockchain* elle-même ne semble pas pouvoir leur être reprochée[35]. La responsabilité des mineurs apparaît, en revanche, majoritairement écartée par la doctrine. Il est vrai qu'ils ne jouent aucun rôle dans la détermination de la finalité des traitements opérés sur la chaîne, en se contentant de valider les opérations effectuées par les utilisateurs[36]. Un rapport envisage cependant la responsabilité des nœuds[37]. Participant à la validation des blocs, ils peuvent également, s'ils sont majoritaires, modifier les règles de la *blockchain*. Ils ont donc une incidence importante sur les moyens du traitement et, lorsqu'ils valident une opération, déterminent effectivement sa finalité.

De telles divergences, ne permettant pas de proposer une solution satisfaisante, ont conduit la CNIL à se prononcer. Contre toute attente, elle qualifia les utilisateurs de responsables de traitement[38]. S'ils déterminent la finalité du traitement qu'ils opèrent sur la *blockchain*, leur incidence sur les moyens demeure minime[39] et ils ne semblent pas suffisamment contrôler la chaîne pour endosser une telle responsabilité. Surtout, une telle

---

[33] Les finalités du traitement opéré par les plateformes sont, en effet, spécifiques en concernant la lutte contre le blanchiment et les terrorisme, d'une part ; l'exécution des relations contractuelles conclues entre elles et les utilisateurs, d'autre part. La lecture de la politique de confidentialité de la plateforme d'achat *Coinhouse* confirme une telle interprétation : https://www.coinhouse.com/fr/politique-de-confidentialite/.

[34] M. POPPE, « Quelle relation entre la protection des données à caractère personnel et la blockchain ? », *op. cit*.

[35] En outre, ces concepteurs ne sont pas toujours identifiables en ce qu'ils usent de pseudonymes ou de logiciels libres : H. CHRISTODOULOU, « Les nouvelles technologies à l'origine de l'évolution contractuelle », Comm. com. électr., n°11, 2020, Étude 20.

[36] Ils pourraient, en revanche, être qualifiés de sous-traitants : CNIL, *Blockchain : Premiers éléments d'analyse de la CNIL*, *op. cit*., p. 2 ; European Parliament, *Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law ?,* July 2019, p. 46 ; T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *op. cit*.

[37] European Parliament, *Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law ?, op. cit*., p. 46. Le Professeur Douville a également pu envisager cette hypothèse tout en démontrant ses limites : T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *op. cit*.

[38] CNIL, *Blockchain : Premiers éléments d'analyse de la CNIL*, *op. cit*., p. 2. Le parlement européen semble également privilégier cette hypothèse : Parlement européen, Rapport sur la chaîne de blocs : une politique commerciale tournée vers l'avenir, 2018/2085(INI), 27 nov. 2018, §23.

[39] European Parliament, *Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law ?, op. cit*., p. 48.

lecture n'apparaît pas acceptable en ce qu'elle suppose qu'une même personne puisse cumuler les qualités de responsable de traitement et de personne concernée[40]. Consciente de cette difficulté, la CNIL l'écarte en invoquant l'exception tenant à l'usage domestique[41] selon laquelle le RGPD n'a pas à s'appliquer aux traitements réalisés « dans le cadre d'une activité strictement personnelle ou domestique »[42]. Or, selon le dispositif de l'instrument, il s'applique en revanche aux responsables fournissant les moyens de traiter les données pour de telles activités[43]. Partant, si un particulier utilise la *blockchain* pour transférer des *bitcoins*, l'opération est certes personnelle mais se trouve permise par une technologie devant répondre au RGPD. Par ailleurs, l'assertion de la CNIL apparaît contraire à la jurisprudence de la Cour de justice de l'Union européenne[44] qui écarte l'exception susvisée lorsque les données sont « rendues accessibles à un nombre indéfini de personnes »[45]. Publique par nature, la *blockchain* semble permettre un tel accès, peu important que les données demeurent cryptées. L'exception ne semble donc pas applicable et les qualités de personne concernée et de responsable pourraient donc, en pratique, se cumuler. Or comment peut-on être, à la fois, débiteur et créancier de la même obligation ? En droit français, la confusion de ces qualités entraîne l'extinction de l'obligation[46], du moment qu'il s'agit d'un droit de créance[47]. Si la nature des démembrements du droit à la protection des données reste floue[48], il est certain qu'admettre un tel cumul porte atteinte à son essence, la personne concernée n'apparaissant pas suffisamment armée pour veiller à la protection de ses intérêts.

À l'issue de cette présentation, les responsabilités des nœuds et des utilisateurs semblent majoritairement admises. Toutefois, au regard de leurs limites, ne conviendrait-il pas de les qualifier, ensemble, de coresponsables de traitement ? Permise par le RGPD[49], cette

---

[40] I. BELIC, *Data Protection Challenges of public permissionles blockchains in relation to the GDPR*, Tilburg University, June 2018, p. 36.
[41] CNIL, *Blockchain : Premiers éléments d'analyse de la CNIL*, *op. cit*., p. 3.
[42] Art. 2§2, c), Règlement (UE) 2016/679, précité.
[43] Cons. 18, *Ibid*.
[44] European Parliament, *Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law ?, op. cit*., p. 12.
[45] CJCE, 6 nov. 2003, *Bodil Lindqvist*, Aff. C-101/01, §47 – D., 2004, 1062, obs. L. Burgogne-Larsen ; Comm. com. électr., 2004, 4, 46, comm. R. Munos ; CJUE, gde ch., 16 déc. 2008, *Tietosuojavaltuutettu c/ Satakunnan Markkinapörssi Oy, Satamedia Oy*, Aff. C-73/07, §§43-44 – RSC, 2009, 197, obs. L. IDOT ; CJUE, 4ème ch., 11 déc. 2014, *František Ryneš c/ Úřad pro ochranu osobních údajů*, Aff. C-212/13, §§26 et s. – Europe, 2, 2015, 46, comm. F. Gazin.
[46] Art. 1349, Code civil.
[47] Y. DAGORNE-LABBE, « Confusion » *in Répertoire de droit civil*, Dalloz, janv. 2017, n°5.
[48] V. pour une application de la qualification de droit de créance, L. PAILLER, « L'article 8 de la Charte des droits fondamentaux de l'Union européenne - Quel apport à la protection des données à caractère personnel ? », Légipresse, 2015, p. 593.
[49] En effet, le responsable de traitement est défini comme celui qui « seul ou conjointement avec d'autres » détermine les finalités et les moyens du traitement : Art. 4§7, Règlement (UE) 2016/679, précité.

qualification nécessite de démontrer que les décisions tenant à la finalité et aux moyens résultent d'une intention commune ou, au moins, convergente. Il n'est donc pas indispensable que les intervenants poursuivent des finalités identiques du moment qu'elles apparaissent étroitement liées ou complémentaires[50]. De même, les moyens n'ont pas à être déterminés par l'ensemble des participants si chacun d'eux à une réelle influence sur ces derniers[51]. Si, à certains égards, la *blockchain* témoigne d'une telle œuvre commune, le RGPD exige toutefois des coresponsables qu'ils définissent « de manière transparente leurs obligations respectives » et qu'existe une claire répartition des responsabilités de chaque intervenant[52]. Protégeant la personne concernée, en favorisant la transparence du système, cette condition est ignorée par les acteurs de la *blockchain*[53]. De surcroît, admettre cette coresponsabilité n'apparaît pas susceptible d'assurer la protection des données traitées dans la *blockchain*. En effet, les nœuds et les utilisateurs restent instables et il est très difficile de les identifier et, *a fortiori*, de les localiser[54]. D'autre part, même si leur responsabilité était jugée solidaire en permettant à la personne concernée de s'adresser à un seul d'entre eux, celui-ci ne n'aura pas accès aux données en clair[55] et n'aura donc aucune emprise sur celles-ci[56].

Finalement, aucun sujet ne semble avoir le contrôle des données traitées sur la *blockchain*[57]. Extrêmement gênante, cette situation empêche la personne concernée d'exercer ses droits et lui cause, *de facto*, un préjudice. De même, celui-ci pourrait naître d'une atteinte à la sécurité de la *blockchain* qui emporterait des vols ou des destructions de données. Qu'il s'agisse de l'exercice des droits, qui est contrarié, ou d'une atteinte plus directe à la donnée, à qui la personne concernée peut-elle s'adresser pour obtenir la cessation de l'atteinte et la réparation de son préjudice ? Si tout contrôle de la *blockchain*, au sens du RGPD, semble interdit, en va-t-il de même pour les actions en responsabilité qu'il prévoit ? À la lecture de ses

---

[50] EDPB, *Guidelines 07/2020*, *op. cit*., p. 19.
[51] CJUE, gde ch., 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH*, Aff. C-210/16, §43 – RDC, 4, 2018, 555, obs. A. Danis-Fatôme ; Comm. com. électr., 9, 2018, 67, comm. N. Metallinos ; JCP G, 28, 2018, 810, note D. Berlin ; Europe, 8-9, 2018, 298, comm. D. Simon – CJUE, gde ch., 29 juill. 2019, *Fashion ID GmbH & Co. KG c/ Verbraucherzentrale NRW eV*, Aff. C-40/17, §70 – RTD Eur., 2020, 319, obs. F. Benoît-Rohmer ; Dalloz IP/IT, 2020, 126, obs. T. Douville ; Europe, 10, 2019, 377, comm. F. Péraldi-Leneuf ; Comm. com. électr., 11, 2019, 71, comm. N. Metallinos ; JCP G, 40, 2019, 993, note F. Mattatia.
[52] Art. 26 et Cons. 79, Règlement (UE) 2016/679, *op. cit.*
[53] J. DEROULEZ, « Quel responsable de traitement ? », *op. cit.*
[54] T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *op. cit.* ; M. FINCK, « Blockchains and Data Protection in the European Union », Max Planck Institute for Innovation & Competition Research Paper, No. 18-01, 30 Nov. 2017, p. 17.
[55] European Parliament, *Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law ?, op. cit*., p. 72.
[56] M. FINCK, « Blockchains and Data Protection in the European Union », *op. cit*., p. 17.
[57] *Ibid*., p. 52.

dispositions, celles-ci semblent, une fois encore, subordonnées à l'identification d'un responsable de traitement, ou d'un sous-traitant agissant en dehors de ses instructions[58], ou à la caractérisation d'une responsabilité conjointe[59].

Une analyse casuistique est indispensable et nulle réponse statique valant pour toutes les *blockchains* ne saurait être apportée. Si l'identification d'un responsable de traitement semble, dans l'absolu, permise, elle nécessitera une recherche extrêmement complexe qui incombera à la personne concernée. Or, n'est-il pas irréaliste de lui imposer une telle charge ? Celle-ci risque, en effet, de se décourager et de renoncer à faire valoir ses droits. Dès lors, à défaut d'identifier les responsables de la *blockchain*, il s'agit de s'interroger sur leur éventuelle responsabilisation (**II**).

## II. L'unique alternative : la responsabilité des acteurs de la *blockchain*

Le droit à la protection des données semble fragile sur la *blockchain*, en dépit de l'affirmation de la neutralité technologique du RGPD. La responsabilité civile, ayant fait la preuve de sa malléabilité, pourrait venir corriger les faiblesses de ce texte et, au moins temporairement, sauvegarder ce droit fondamental.

Alors que le régime des produits défectueux semble peu adapté (**A**), la responsabilité générale du fait des choses se révèle d'un grand secours (**B**).

### A. Les produits défectueux : une fausse bonne idée

En s'éloignant du RGPD et, partant, de l'impératif d'identifier un responsable de traitement, l'application du régime des produits défectueux pourrait être envisagée[60]. Au-delà du triptyque classique de la responsabilité civile, il conviendra alors de démontrer que la *blockchain*, pouvant s'analyser comme un produit[61], présente un défaut qui serait imputable à un producteur. Là encore, l'identification de ce protagoniste risque de se révéler périlleuse. Elle

[58] Art. 79 et 82, Règlement (UE) 2016/679, précité.
[59] Art. 82§§4 et 5, *Ibid*.
[60] Art. 1245 à 1245-17, Code civil ; Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux, JO L 210 du 7 août 1985.
[61] En ce sens, la *blockchain* semble pouvoir être considérée comme un « produit » au sens de l'article 1245-2 du Code civil, celui-ci s'appliquant aux choses incorporelles : C. CAILLE, « Responsabilité du fait des produits défectueux » *in Répertoire de droit civil*, Dalloz, 2018, n°29.

se confrontera à l'anonymat des concepteurs[62] et, même à considérer que la responsabilité des intermédiaires puisse être recherchée[63], la verticalité du régime des produits défectueux générera des difficultés analogues à celles rencontrées dans le cadre du RGPD[64]. Surtout, la condition tenant à la défectuosité du produit apparaît particulièrement compliquée à satisfaire. Est considéré défectueux tout produit qui « n'offre pas la sécurité à laquelle on peut légitimement s'attendre »[65] en tenant compte, notamment, de l'usage raisonnablement attendu et du moment de sa mise en circulation. Dès lors, le producteur ne saurait se voir reprocher un défaut qui ne pouvait être anticipé par des mesures de sécurité qui n'existaient pas lors de la mise en circulation du produit[66]. Par ailleurs, le défaut doit préexister à cette dernière[67] ou, à tout le moins, ne devait pas pouvoir être décelé en l'état des connaissances scientifiques et techniques[68]. Au regard de la complexité de la technologie *blockchain*, il y a fort à penser pour que le défaut ne puisse être anticipé[69], voire qu'il naisse de sa seule utilisation, d'autant que les nœuds du réseau sont habilités à modifier l'architecture et les règles de fonctionnement de la chaîne[70].

Le régime des produits défectueux, dont la verticalité fait écho au RGPD, ne semble pas idéal. Le régime général de la responsabilité du fait des choses, ayant déjà fait la preuve de sa plasticité, pourrait alors être envisagé.

### B. Un régime à exploiter : la responsabilité du fait des choses

[62] H. CHRISTODOULOU, « Les nouvelles technologies à l'origine de l'évolution contractuelle », *op. cit*. ; H. de VAUPLANE, « Le droit civil à l'épreuve de la blockchain », Revues des Juristes de Sciences Po, n°16, 2019, act.1.
[63] Conformément aux articles 1245-6 et 1245-7 du Code civil.
[64] V. *supra*.
[65] Art. 1245-3, Code civil ; Art. 6, Directive 85/374/CEE, précitée.
[66] *Ibidem*.
[67] Art. 1245-10, 2°, Code civil ; Art. 7, Directive 85/374/CEE, précitée.
[68] Art. 1245-10, 4°, *Ibid*. V. not. au sujet du risque de développement, F. TERRE et al., *Droit civil. Les obligations*, Dalloz, coll. « Précis », 2018, n°1230 ; O. BERG, « La notion de risque de développement en matière de responsabilité du fait des produits défectueux », JCP G, n°27, 1996, doctr. 3945 ; P. LE TOURNEAU, « De l'application de la loi du 19 mai 1998 sur la responsabilité du fait des produits défectueux, notamment quant au "risque de développement" », JCP G, n°48, 2000, II 10429.
[69] L. GODEFROY, « Le code algorithmique au service du droit », D., 2018, p. 734.
[70] V. *supra*.

La responsabilité du fait des choses[71] pourrait, éventuellement, offrir un palliatif intéressant. Fondée sur la théorie du risque, elle semble particulièrement adaptée à la technologie disruptive qu'est la *blockchain*. Néanmoins, là encore, certaines corrections devront être apportées.

Tout d'abord, il faudrait écarter définitivement le régime des produits défectueux, sous peine d'empêcher la victime de se fonder sur la responsabilité du fait des choses[72]. Ensuite, il conviendrait d'admettre que cette dernière puisse s'appliquer aux choses incorporelles[73], ce que les développements informatiques et technologiques justifient plus que jamais[74]. Enfin, les conditions nécessaires à son engagement devraient être appréciées à l'aune des particularités de la *blockchain*. À cet égard, si la démonstration du préjudice[75] et du lien de causalité ne devrait pas soulever de difficultés particulières, en va-t-il de même quant au fait de la chose ? En considérant que la *blockchain* constitue une chose inerte, il conviendra de rapporter la preuve de son rôle actif dans la réalisation du dommage[76]. Un défaut de sécurité, même postérieur à son entrée en circulation, voire même l'incompatibilité intrinsèque de cette technologie avec les règles du RGPD pourraient, *a priori*, suffire à établir le critère de l'anormalité.

Si la mise en œuvre de la responsabilité du fait des choses semble permise, il conviendra toutefois d'identifier un responsable, le gardien, en recherchant la personne ayant l'usage, le contrôle et la direction de la *blockchain* au moment du dommage[77]. Un tel exercice promet d'être périlleux et la présomption pesant sur le propriétaire[78] n'apportera aucun secours. De même, la distinction opérée entre la garde de la structure et du comportement ne constitue pas une alternative satisfaisante. En effet, alors que les concepteurs peuvent, *a priori*, être considérés comme les gardiens de la structure, ils abandonnent ensuite cette dernière aux nœuds qui ont la possibilité de la modifier. Serait-il possible, enfin, d'imaginer une garde collective qui incomberait à l'ensemble des intervenants ? Si le principe reste l'unicité, la jurisprudence

---

[71] Art. 1242, *Ibid*.

[72] En effet, la victime ne peut se fonder sur la responsabilité du fait des choses dans le cas où son action relèverait du régime des produits défectueux, quand bien même l'exonération pour risque de développement serait applicable : CJCE, 5ème ch., 25 avr. 2002, *María Victoria González Sánchez*, Aff. C-183/00 – RTD Civ., 2002, 523, obs. P. Jourdain ; D., 2002, 2462, obs. C. Larroumet ; RTD Civ., 2002, 868, obs. J. Raynard ; CJCE, gde ch., 10 janv. 2006, *Skov Æg c/ Bilka Lavprisvarehus A/S*, Aff. C-402/03 – RTD Civ., 2006, 333, obs. P. Jourdain ; D., 2006, 1259, obs. C. Nourissat.

[73] Le Projet de réforme du droit de la responsabilité civile exclue les choses incorporelles : Art. 1243, al. 1.

[74] L. GRYNBAUM, « Responsabilité du fait des choses inanimées », *Répertoire de droit civil*, Dalloz, 2011, n°142 ; A. SIGNORILE, « Vers une responsabilité du fait des choses incorporelles à l'aune du numérique ? (Partie I) », Revue Lamy Droit de l'Immatériel, n°159, 2019. V. contra., A. LUCAS, « La responsabilité des choses immatérielles », *Mél. Catala*, Litec, 2001, pp. 817 et s.

[75] Résultant d'une atteinte au droit à la protection des données, celui-ci pourrait être moral et/ou matériel.

[76] Cass. 2ème Civ., 17 févr. 2005, n° 01-15.666 – JCP G, 2005, I, 149, obs. G. Viney.

[77] Cass. civ. ch. réunies, 2 déc. 1941.

[78] Cass. ch. mixte, 4 déc. 1981 – JCP, II, 1982, 19748, note H. Mazeaud.

admet qu'une garde commune soit caractérisée dès lors que des pouvoirs de droit ou de fait se trouvent exercés au même titre sur la chose ou, dans un souci d'indemnisation, lorsque le gardien ne peut être identifié aisément[79]. Séduisante, cette solution pourrait toutefois conduire à exclure la réparation dans le cas où la victime compte parmi les cogardiens[80]. Pour contrer cette difficulté, la garde devrait être réputée partagée entre les concepteurs, les nœuds et les mineurs, à l'exception des utilisateurs. Face à l'opacité de la *blockchain*, une présomption de garde commune pourrait être admise tout en autorisant un recours subrogatoire vers le véritable gardien s'il peut être identifié. Protégeant la personne concernée, cette solution renouerait avec la logique du RGPD tout en demeurant cohérente avec la théorie du risque fondant la responsabilité du fait des choses. Plus loin encore, la logique d'indemnisation pourrait gommer l'intérêt d'identifier un responsable. Il est en ce sens permis d'imaginer la création d'un fonds de garantie qui, à titre subsidiaire, serait chargé d'indemniser les dommages générés par la *blockchain*. Alimenté par l'ensemble de ses intervenants, il contribuerait à l'effectivité du droit à la protection des données tout en ne constituant pas une charge excessive sur les acteurs de cette technologie inédite.

Si de nombreuses interrogations demeurent, la responsabilité civile pourrait offrir un palliatif au RGPD avant que ne soit définitivement tranchée la question de sa compatibilité avec la *blockchain*. Pour cela, il conviendrait de modeler les notions de responsable de traitement ou de responsabilité conjointe et renoncer à la prétendue neutralité technologique de cet instrument européen.

[79] V. par exemple, Cass. 2ème Civ., 13 janv. 2005, n°03-12.884
[80] Cass. 2ème Civ., 20 nov. 1968, Bull. civ. II, n°77 – RTD civ., 1969, 335, obs. Durry – Cass. 2ème Civ., 25 nov. 1999, n°97-20.343.