Cryptomonnaies et RGPD

Sonia Daoui
Avocat au barreau de Paris

&

Marc Lempérière
Avocat aux barreaux de Paris et de New York, associé du cabinet Almain

Thomas Fleinert-Jensen
Avocat au barreau de Paris, associé du cabinet Almain

Si la notion de blockchain reste encore méconnue dans l'esprit du grand public, l'une de ses applications pratiques fait régulièrement la une des journaux et revêt un caractère plus palpable : il s'agit des cryptomonnaies.

C'est par des blockchains que les cryptomonnaies permettent d'acheter des biens et services réels ou virtuels, de réaliser des paiements en *peer to peer* ou d'investir de manière plus ou moins spéculative.

Techniquement, les opérations d'achat, de vente et d'échange de cryptomonnaies sont réalisées par la création de nouveaux « blocs » de données contenant des informations sur la transaction. Les blocs sont envoyés aux participants à la blockchain, appelés « mineurs ». Ces derniers doivent valider le bloc au regard d'un algorithme prédéfini, dit « mécanisme de consensus ». Une fois validé, le bloc est ajouté à la chaîne. Le mineur est généralement rémunéré pour sa participation à la blockchain, par la création de nouvelles unités de cryptomonnaie.

Des copies du registre de chaque blockchain sont conservées sur des ordinateurs appelés des « nœuds » qui peuvent être disséminés dans le monde entier. C'est l'une des grandes différences des blockchains avec les bases de données classiques qui sont centralisées et, éventuellement, répliquées une ou deux fois pour des simples raisons de sauvegarde.

S'agissant de transactions en cryptomonnaies effectuées *in fine* par ou pour des personnes physiques, elles sont susceptibles de traiter des données personnelles. À ce titre, elles sont soumises aux règles applicables en matière de protection de la vie privée et, en Europe, plus particulièrement au règlement général sur la protection des données (RGPD) applicable depuis le 25 mai 2018[1].

La notion de donnée à caractère personnel est vaste. Elle est définie par le RGPD dans les termes suivants[2] : « Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Quand bien même une transaction en cryptomonnaie serait anonyme en elle-même, c'est-à-dire que le bloc ne ferait pas mention du nom d'une personne physique, elle serait néanmoins soumise au RGPD s'il est techniquement possible d'identifier une telle personne physique concernée par la transaction. Les données à caractère personnel comprennent les numéros d'identification, les données de localisation et les identifiants en ligne.

Le règlement s'applique au traitement de données effectué par des responsables du traitement ou aux sous-traitants établis sur le territoire de l'Union européenne, si le traitement des données intervient effectivement à l'intérieur de celle-ci. Il couvre également le traitement de données à caractère personnel de personnes situées sur le territoire de l'Union européenne par des responsables du traitement ou des sous-traitants n'ayant aucune présence physique dans celle-ci, mais proposant des biens ou des services à des personnes situées dans l'Union européenne ou suivant

1. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
2. Art. 4 (1) du RGPD.

les comportements de ces personnes si ces comportements se produisent au sein de l'Union.

Le RGPD a souvent été présenté comme indépendant de la technologie. Le règlement a néanmoins été conçu en gardant à l'esprit la base de données centralisée classique où il existe presque toujours une entité qui détermine la finalité et les moyens du traitement, met en place les systèmes correspondants et traite les données[3].

Les blockchains, et notamment les transactions en cryptomonnaies, remettent en cause ce paradigme puisqu'elles sont structurées de façon décentralisée. À qui une personne physique doit-elle s'adresser pour faire respecter ses droits au titre du RGPD dans le cadre d'une transaction en cryptomonnaies ? Comment rendre effectif le droit à l'oubli prévu par le RGPD alors que les données inscrites sur une blockchain sont par nature ineffaçables ? Telles sont les principales questions soulevées par les cryptomonnaies qui seront successivement examinées, avant d'aborder quelques autres exigences du RGPD. En outre, la question de la protection des données personnelles dans le cadre des transactions en cryptomonnaie ne semble pas non plus résolue par les cryptomonnaies anonymes dont les caractéristiques présentent des frictions avec les exigences KYC/AML/CFT propres au secteur financier.

I. Qui est responsable de la conformité des échanges en cryptomonnaies avec le RGPD ?

En langage RGPD, répondre à cette question revient à déterminer qui est le « responsable de traitement ». Le RGPD définit le responsable du traitement de la manière suivante : « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement » de données à caractère personnel[4].

Le rôle du responsable du traitement est central dans la protection des données personnelles. C'est lui qui doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir la conformité du traitement des données aux règles de protection du RGPD. À ce titre, le responsable du traitement est responsable des dommages causés à toute personne concernée par le traitement. Il s'expose à des amendes substantielles en cas de non-conformité, pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour les entreprises, le montant le plus élevé étant retenu.

Indépendamment des amendes administratives, les États membres de l'Union européenne peuvent également appliquer d'autres sanctions nationales. En France, par exemple, la violation des règles de protection des données personnelles est punie de peines allant jusqu'à cinq ans d'emprisonnement et de 300 000 euros d'amende pour les personnes physiques, montant quintuplé pour les personnes morales.

La détermination du responsable de traitement en matière de cryptomonnaies ne va pas de soi. Autant il est relativement aisé d'identifier l'entité responsable du traitement des données dans le cadre classique de gestions de données centralisée telle qu'elle se pratique habituellement dans les systèmes informatiques, autant cet exercice est délicat dans un système décentralisé de blockchain qui est sous-jacent aux cryptomonnaies.

L'entrée en vigueur du RGPD a été accompagnée de nombreux commentaires sur sa nature présumée inconciliable avec la blockchain, en particulier sur les blockchains publiques et sans autorisation. Intégrer la blockchain dans le modèle centralisé du RGPD est souvent perçu comme une tentative de quadrature du cercle.

La communication de la CNIL du mois de septembre 2018 donne un éclairage bienvenu de la part d'une autorité de régulation[5]. Sur la base de la définition du RGPD, la CNIL considère que les participants à la blockchain qui ont un droit d'écriture sur la chaîne et pouvant décider de soumettre des données à validation par des mineurs peuvent être considérés comme des responsables du traitement.

Plus précisément, la CNIL considère qu'un participant est un responsable du traitement :

- lorsqu'il s'agit d'une personne physique qui traite des données à caractère personnel en lien avec une activité professionnelle ou commerciale ; et
- lorsqu'il s'agit d'une personne morale qui inscrit des données personnelles sur une blockchain.

Par exemple, la CNIL indique que le notaire qui enregistre l'acte de propriété d'un client sur une blockchain est considéré comme responsable du traitement. De même, lorsqu'une banque enregistre des données client sur une blockchain, elle doit être considérée comme responsable du traitement.

S'agissant plus particulièrement des cryptomonnaies, la CNIL considère que n'est pas responsable de traitement la personne physique qui procède à la vente ou à l'achat de Bitcoins pour son propre compte. En effet, selon l'article 2.b) du RGPD, ce dernier n'est pas applicable au traitement de données personnelles effectué par une personne physique dans le cadre d'une activité

3. L'Observateur-Forum des blockchains dans l'Union européenne, « Blockchain et le RGPD », 17 (16 octobre 2018), https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.
4. Art. 4 du RGPD.
5. CNIL, « Blockchain, Premiers éléments d'analyse de la CNIL », septembre 2018.

strictement personnelle ou domestique. En revanche, doit être considérée comme responsable de traitement la personne physique qui procède à de telles opérations dans le cadre d'une activité professionnelle ou commerciale, pour le compte d'autres personnes physiques.

La CNIL n'en dit pas plus, mais ces considérations pourraient laisser penser qu'un commerçant qui ferait payer ses prestations en cryptomonnaies à travers une app serait responsable de traitement des données personnelles. Ce serait donc ce commerçant qui devrait veiller à la protection de ses données conformément au RGPD et qui en répondrait à l'égard des autorités de contrôle.

En revanche, les nœuds de validation ne sont pas considérés par la CNIL comme des responsables de traitement, car ils ne déterminent pas les finalités et les moyens du traitement des données à caractère personnel. Cette position reflète la vision commune de la communauté blockchain[6].

Le débat n'est toutefois pas clos. Une récente étude sur les rapports entre la blockchain et le RGPD réalisée pour le Parlement européen mettait en doute que le principe d'exception domestique (« *household exemption* ») s'applique au traitement des données personnelles dans une blockchain[7]. L'étude rappelle la jurisprudence de la Cour de justice de l'Union européenne qui adopte une interprétation restrictive de l'exemption domestique. Si les données personnelles collectées deviennent accessibles à un nombre indéfini de personnes, le principe ne s'applique pas. Les blockchains publiques sans permission permettent une telle diffusion, ce qui suggérerait que l'exception domestique ne leur serait pas applicable.

On remarquera également que plusieurs régulateurs nationaux ont d'ores et déjà demandé des comptes à l'association Libra quant à la protection des données personnelles, ce qui pourrait conduire à une extension de la définition de responsable de traitement dans les blockchains.

L'association Libra est un regroupement d'entreprises, d'organisations à but non lucratif et d'institutions universitaires qui a pour objet de faciliter le fonctionnement de la blockchain Libra, de coordonner l'entente entre les nœuds de validation du réseau et gérer la réserve d'actifs réels qui sous-tend cette cryptomonnaie[8]. Les membres fondateurs incluent des noms comme Mastercard, PayPal, Visa, Facebook, Spotify et Vodafone. L'association Libra gère ainsi la structure de la blockchain Libra.

Les régulateurs nationaux d'Albanie, d'Australie, du Burkina Faso, du Canada, des États-Unis, du Royaume Uni et de l'Union européenne ont publié une déclaration commune au mois d'août 2019 aux termes de laquelle ils faisaient part de leurs inquiétudes sur la protection des données personnelles dans le cadre du projet Libra. Les régulateurs ont partagé une liste de questions sur la conformité de Libra avec les règles de protection des données personnelles. Ils ont par exemple voulu savoir comment les participants allaient fournir aux utilisateurs une information claire sur l'utilisation de données personnelles et limiter la collecte de telles informations au strict minimum. Ils ont également demandé comment l'association Libra allait s'assurer que tous les sous-traitants de données personnelles allaient être identifiés et allaient se conformer à leurs obligations de protection.

Les questions posées par les régulateurs concernent les responsabilités classiques des responsables de traitement. Or, les régulateurs les ont adressées à l'association Libra, à Calibra, filiale de Facebook et à tout futur fournisseur de portefeuilles (*wallet providers*). Que Calibra et les fournisseurs de portefeuilles soient considérés comme des responsables de traitement, cela se conçoit dans la mesure où ils ont un droit d'écriture sur la chaîne et peuvent décider de soumettre des transactions en Libra à des mineurs. On rejoint à cet égard l'analyse de la CNIL. Il est en revanche plus frappant que les régulateurs s'adressent à l'association Libra elle-même qui n'est responsable que de la structure de la blockchain. Est-ce à dire qu'elle sera également considérée comme responsable de traitement ? L'avenir le dira.

II. Cryptomonnaies et droit à l'oubli

En vertu du RGPD, toute personne concernée a le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel la concernant. Cette règle est énoncée par l'article 17 du règlement aux termes duquel : « La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais […] ».

L'article 17 dresse ensuite la liste des cas où ce droit trouve application, notamment celui où les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, et le cas où la personne concernée retire son consentement pour le traitement de ses données à caractère personnel, lorsque le consentement est le fondement juridique du traitement des données.

À l'inverse, les blockchains sont basées sur le principe d'immutabilité, selon lequel des informations peuvent être ajoutées via de nouveaux blocs mais ne peuvent pas être supprimées, ou à tout le moins seulement au prix de manipulations techniques lourdes et sous condition

6. L'Observatoire-Forum des blockchains de l'Union européenne, *supra*, note 4, p. 17.
7. « Blockchain and the General Data Protection Regulation », European Parliamentary Research Service, juillet 2019.
8. « Une introduction à Libra », Livre blanc, www.libra.org.

d'obtenir un consensus suffisant au sein de la chaîne. Il s'agit là d'ailleurs de l'un des principaux intérêts de la blockchain qui vise à renforcer la confiance en l'intégrité des données qui y sont enregistrées. Toute donnée personnelle qui serait enregistrée sur une blockchain ne pourrait donc pas être effacée. Il en est particulièrement ainsi pour les transactions en cryptomonnaies, qui ne seraient donc par nature pas compatibles avec les règles du RGPD.

Dans son analyse de septembre 2018, la CNIL reconnaît qu'il est techniquement impossible de donner suite à une demande d'effacement lorsque les données à caractère personnel sont enregistrées dans la blockchain.

L'étude réalisée pour le Parlement européen souligne également la difficulté de procéder à l'effacement des données enregistrées sur blockchain[9]. Elle relève toutefois que la notion d'effacement des données n'est pas définie par le RGPD et que certaines jurisprudences de la Cour de justice de l'Union européenne pourraient laisser penser que le responsable de traitement se doit seulement d'assurer un résultat aussi proche que possible de la destruction des données dans la limite de ses moyens techniques[10], même si d'autres semblent assimiler l'effacement à la destruction[11]. Il reste donc à la jurisprudence d'affiner la définition de l'effacement de données, ce qui ne sera pas sans influence sur la compatibilité des blockchains avec le RGPD.

S'agissant plus particulièrement des cryptomonnaies, elles sont parfois présentées comme étant des monnaies anonymes. Pour le Bitcoin par exemple, chacun est en mesure de vérifier la chaîne des transactions par des moyens simples, et rien ne permet à première vue de relier les Bitcoins à des individus. En réalité, il ne serait pas impossible techniquement de retrouver les parties derrière une transaction, fût-ce avec des moyens coûteux[12]. Le Bitcoin peut donc être considéré comme procédant au traitement de données personnelles, ce qui laisse ouverte la question de leur effacement.

La plupart des autres crypto-monnaies, et notamment l'Ethereum, le Ripple, le Bitcoin cash, le Litecoin, le Stellar, le Cardano, le IOTA ou le NEO, sont dans la même situation : même s'il est difficile en pratique d'identifier une personne à l'origine d'une transaction, il est techniquement possible de révéler l'identité des parties à la transaction par l'emploi de moyens certes complexes et coûteux. Au vu de la jurisprudence sur cette question, il semble difficile d'arguer que les techniques avancées de pseudonymisation utilisées par ces crypto-monnaies leur permettre de soutenir qu'elles ne traitent pas des données personnelles.

D'autres essayeraient de pousser la pseudonymisation plus loin. Tel serait le cas de Monero avec la technique du *Ring Confidential Transactions* et des *stealth adresses*, ou encore de Dash avec la technique *PrivateSend* (cf. section IV ci-après).

S'agissant de Libra, la blockchain devrait utiliser des pseudonymes en permettant à ses utilisateurs de détenir une ou plusieurs adresses qui ne sont pas liées à leur identité réelle[13]. Il n'est pas certain à ce stade que le lien avec ces utilisateurs ne puisse pas être effectué, et que certaines données enregistrées n'aient donc pas le caractère de données personnelles.

Quoi qu'il en soit, faute de pouvoir techniquement effacer des données personnelles enregistrées dans le cadre de transactions en cryptomonnaies, il est envisageable de recourir à des méthodes qui produisent un effet proche, tout en sachant qu'elles ne satisfont pas nécessairement les règles du RGPD.

Tel est le cas selon la CNIL lorsque les données sont enregistrées dans la blockchain par hachage ou par un cryptage à la pointe de la technologie. Si, par exemple, la clé privée est supprimée, il n'existera en pratique aucun risque en ce qui concerne la confidentialité des données à caractère personnel.

La CNIL demeure prudente : il reste à déterminer si de tels moyens peuvent être considérés comme équivalant à un droit d'effacement. En tout état de cause, elle recommande de ne pas enregistrer de données à caractère personnel directement sur la blockchain sans cryptage. En raison du principe de protection des données dès la conception exigée par le RGPD[14], les données à caractère personnel non protégées doivent être enregistrées ailleurs, par exemple dans la base de données des utilisateurs du réseau, où elles peuvent être effacées conformément au règlement. La blockchain ne contiendra alors que des informations indiquant que ces données se trouvent dans la base de données.

De même, afin de minimiser le problème de l'effacement, les participants doivent s'en tenir à l'un des principes fondamentaux du RGPD selon lequel le traitement des données à caractère personnel doit être limité à ce qui est nécessaire eu égard aux finalités pour lesquelles elles sont traitées[15]. Sur la base de cette règle, les directives de la CNIL examinent la manière dont les utilisateurs et les nœuds sont identifiés dans les blockchains, ce qui se fait essentiellement par le biais d'une clé publique et d'une clé privée confidentielle. L'identification publique des utilisateurs et des nœuds est toujours visible car il s'agit d'une exigence technique pour les blockchains. Selon la CNIL,

9. « Blockchain and the General Data Protection Regulation », European Parliamentary Research Service, juillet 2019, pp. 74 et s.
10. C.J.U.E., 13 mai 2014, *Google Spain*, affaire C-131/12.
11. C.J.U.E., 20 décembre 2017, *Peter Nowak*, affaire C-434/16.
12. Parlement européen, « Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion », juillet 2018, pp. 33 et s.
13. « Une introduction à Libra », Livre blanc, p. 6, www.libra.org.
14. Art. 25.
15. Art. 5 (1) c.

il n'existe aucun moyen de réduire davantage cette identification.

Une autre analyse basée sur une lecture attentive de l'article 17 du RGPD pourrait être faite en conciliant le droit à l'effacement avec la blockchain. Le droit à l'oubli n'existe en effet que dans six cas bien définis, dont cinq ne s'appliquent pas à la plupart des opérations de blockchain : (1) Offres de services de la société de l'information à l'intention des enfants de moins de 16 ans ; (2) obligation de supprimer les données conformément au droit national applicable ; (3) traitement illégal des données ; (4) la personne concernée s'oppose au traitement de données qui était légalement fondé sur le fait que ce traitement était nécessaire à l'exercice d'une mission de service public ou aux intérêts légitimes du responsable du traitement ; (5) traitement de données basé sur le consentement.

Le traitement des données pour les services blockchain repose généralement sur le fait que le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution des mesures précontractuelles adoptées à sa demande. Par conséquent, la seule justification s'agissant d'une demande de suppression des données d'une blockchain serait la suivante : les données à caractère personnel ne sont plus nécessaires compte tenu de la finalité pour laquelle elles avaient été collectées.

On pourrait donc faire valoir que, dès lors qu'elle décide de participer à la blockchain, la personne concernée sait que ses données personnelles devront être traitées pendant la durée de la blockchain. Cette durée n'est pas infinie (la loi française interdit les contrats à durée indéterminée), car à un moment donné – dans un avenir plus lointain que ce que nous considérons habituellement mais toujours à un moment donné – tous les dispositifs dans lesquels une partie de la blockchain est stockée seront physiquement détruits et les données seront supprimées.

Par conséquent, on peut considérer que les blockchains conservent des données à caractère personnel pendant toute leur durée et que, jusqu'à la destruction du dernier serveur sur lequel la partie de la blockchain est stockée, les données personnelles de chaque membre de la blockchain sont nécessaires au traitement des données, et donc aucun droit à l'oubli ne s'applique. Le débat passe alors du droit d'être oublié aux obligations d'information des personnes concernées, qui incluent des informations sur la durée de conservation des données.

Dans le cas des transactions en cryptomonnaies, les personnes concernées doivent être informées que leurs données seront conservées jusqu'à la destruction physique du dernier serveur sur lequel la blockchain est stockée. Toutefois, si ces informations ont été fournies, le droit à l'effacement ne s'applique pas nécessairement au traitement de données à des fins de services blockchain. Mais plus généralement, toutes les informations enregistrées sur la blockchain, même cryptées, doivent être réduites au minimum.

III. Quelques autres exigences du RGPD

Les cryptomonnaies se doivent de respecter d'autres règles de protection des données personnelles qui présentent moins de difficultés, à tout le moins pour les blockchains privées ou de consortium, c'est-à-dire celles qui comportent un nombre limité et approuvé de nœuds.

A. Sous-traitance du traitement des données personnelles

Les sous-traitants sont des entités qui traitent des données personnelles pour le compte du responsable du traitement[16]. À ce titre, ils sont soumis à des règles spécifiques en vertu du RGPD.

Les développeurs de *smart contracts* et, dans certains cas, les nœuds de validation peuvent être considérés comme des sous-traitants[17]. Le RGPD exige à cet égard qu'un contrat soit conclu entre le responsable de traitement et les sous-traitants[18]. Le contrat contient un certain nombre de dispositions destinées à protéger le traitement des données à caractère personnel, y compris l'objet et la durée du traitement, la nature et la finalité du traitement, ainsi que le type de données à caractère personnel. Le contrat doit également stipuler que le sous-traitant ne traitera les données à caractère personnel que sur instructions écrites du responsable.

La conclusion d'un tel contrat ne devrait pas être un problème majeur dans la plupart des blockchains privées autorisées. C'est ainsi par exemple que pour Libra, qui dans sa phase de lancement sera une blockchain avec permission, des contrats pourront être conclus avec les nœuds ou les éventuels développeurs de *smart-contrats*.

Il n'en va pas de même pour le Bitcoin qui repose sur une blockchain publique, c'est-à-dire une blockchain où tout un chacun a un accès libre au registre, peut effectuer des transactions et peut devenir mineur. Lorsque la seule exigence d'un nœud de validation consiste à installer un logiciel et à télécharger une copie complète de la blockchain, il est probable qu'aucun accord ne soit jamais conclu avec les utilisateurs du réseau.

16. Art. 28 (1).
17. CNIL, « Blockchain, Premiers éléments d'analyse de la CNIL », septembre 2018.
18. Art. 28 (3).

B. Sécurité du traitement des données personnelles

Parmi les tâches incombant au responsable du traitement des données et au sous-traitant en vertu du RGPD, ils doivent mettre en œuvre les mesures techniques et organisationnelles appropriées, compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement pour assurer un niveau de sécurité approprié au risque pour les droits et libertés des personnes physiques.

Afin que les blockchains soient conformes aux exigences de sécurité du RGPD, la CNIL a notamment recommandé d'évaluer un minimum de mineurs permettant d'assurer l'absence de coalition de 50 % des pouvoirs sur la chaîne. Une telle coalition permettrait en effet de revenir sur une transaction et de remettre ainsi en cause l'intégrité de la blockchain et son immutabilité.

Il s'agit donc d'une exigence primordiale pour maintenir la confiance dans une cryptomonnaie.

Il convient de noter que l'évaluation du niveau de sécurité d'une blockchain évolue en fonction de l'état des connaissances, ce qui risque de poser un réel problème. Une blockchain considérée comme présentant un niveau de sécurité approprié à un instant T peut, du fait de l'apparition de nouvelles technologies, être considérée comme ne présentant plus ce niveau de sécurité approprié. Or, il est techniquement très difficile de modifier les caractéristiques fondamentales d'une blockchain. Le titulaire de cryptomonnaie risque donc, du fait de l'apparition de nouvelles technologies, de voir la valeur de sa cryptomonnaie réduite à zéro du fait de l'incompatibilité avec le RGPD.

C. Droit à l'information

Dans le cadre de transactions en cryptomonnaies, et en vertu du RGPD, le responsable du traitement doit fournir des informations détaillées à la personne concernée au moment où les données à caractère personnel sont obtenues. Le responsable du traitement d'une transaction donnée en cryptomonnaie devra fournir des informations telles que (i) l'identité et les coordonnées du responsable du traitement, (ii) les finalités du traitement pour lesquelles les données à caractère personnel sont destinées et le fondement juridique de ce traitement, (iii) le droit de porter plainte auprès d'une autorité de surveillance et (iv) l'existence d'une prise de décision automatisée.

Si ces informations semblent en effet assez simples à fournir en pratique, il reste que d'autres informations requises semblent plus difficiles à traiter. Le RGPD exige que le responsable du traitement fournisse à la personne concernée des informations sur la période de stockage des données à caractère personnel. Étant donné que les informations ne peuvent pas être supprimées sur les blockchains, cette exigence sera difficile à remplir.

Enfin, les transactions en cryptomonnaie, au même titre que toute inscription de données personnelles sur une blockchain, posent une difficulté au regard du droit d'accès aux données à caractère personnel. L'utilisateur du réseau doit informer la personne concernée de son droit de demander l'accès aux données à caractère personnel, leur rectification ou leur effacement. Seulement, sur la blockchain, les informations ne peuvent pas être rectifiées, mais seulement modifiées en ajoutant un nouveau bloc à la chaîne – les informations ne pouvant pas être effacées.

D. Transfert des données à l'extérieur de l'Union européenne

Il s'agit d'un enjeu important dans le cadre des transactions en cryptomonnaies qui font intervenir des nœuds répartis dans le monde entier. Dès lors que les transactions traitent des données personnelles, celles-ci peuvent se retrouver dans des pays où leur protection pourrait être moins stricte.

Une protection adéquate peut être obtenue par divers moyens définis par le RGPD, notamment :

- des règles d'entreprise contraignantes[19] : ces règles doivent être définies par chaque entreprise concernée et spécifier, entre autres, les transferts de données et l'application des principes généraux de protection des données ;
- des clauses types de protection des données adoptées par la Commission européenne[20] ;
- un code de conduite approuvé[21] : un tel code peut inclure des informations concernant un traitement juste et transparent, la pseudonymisation de données à caractère personnel et l'exercice des droits des personnes concernées.

Ces moyens sont manifestement plus aisés à mettre en œuvre pour les cryptomonnaies fondées sur des blockchains à permission que sur celles fondées sur des blockchains publiques sans permission.

Par ailleurs, s'agissant de certains pays ou territoires non membres de l'Union européenne pour lesquels la Commission européenne a constaté un niveau de protection adéquat, le RGPD permet le transfert de données à caractère personnel sans autorisation spécifique[22]. Par conséquent, le fait que certains utilisateurs ou nœuds de la blockchain soient situés dans de

19. Art. 46 (2) b et art. 47.
20. Art. 93 (2).
21. Art. 40.
22. Art. 45.1.

telles localisations géographiques ne poserait pas de difficulté.

Toutefois, il y a lieu de souligner le nombre restreint de juridictions bénéficiant de décisions d'adéquation : sociétés américaines soumises au « Privacy Shield », Canada, Japon, Île de Man, Argentine, Nouvelle-Zélande, Guernesey, Andorre, Îles Féroé, Suisse et Uruguay.

Il convient aussi de noter que la majorité de ces pays sont petits et que le Privacy Shield, qui autorise les transferts vers des sociétés américaines auto-certifiées, est soumis à une incertitude juridique importante à la suite de la décision de la Haute Cour du tribunal de commerce irlandais de saisir la Cour de justice de l'Union européenne[23] d'une question préjudicielle concernant la légalité de cette décision d'adéquation.

IV. Protection des données personnelles et régulation financière des cryptomonnaies

La traçabilité des transactions effectuées en cryptomonnaies dites « traditionnelles » (Bitcoin, Ethereum), à partir des données inscrites sur les blockchains publiques a soulevé la question de leur confidentialité. La problématique d'anonymisation des transactions a ainsi donné lieu à l'émergence d'une catégorie niche de cryptomonnaies : les « privacy coins » ou cryptomonnaies anonymes.

Dans le cadre de transactions effectuées au moyen de cryptomonnaies anonymes, les informations afférentes aux expéditeurs, receveurs ainsi que celles relatives aux activités du portefeuille sont masquées de manière à les rendre totalement anonymes et non traçables. Plusieurs techniques sont utilisées à cet effet et il convient d'évoquer brièvement celles déployées par les principales cryptomonnaies anonymes ayant cours en termes de capitalisation.

1) Monero (XMR) est basée sur la technologie crypto note. L'anonymat et la non-traçabilité des transactions sont assurés via l'usage de i) « stealth addresses » (clés publiques à usage unique) créées par l'expéditeur pour chaque transaction, ii) « ring signature », permettant de masquer l'identité de l'expéditeur. La technologie « RingCT », introduite en janvier 2017, est une version améliorée des ring signatures qui permet l'obfuscation des montants envoyés.
2) Dash (DASH), mot-valise pour « digital cash », fait usage de la fonction PrivateSend « permettant d'opérer une série de transactions (appelée "mélange") de telle manière qu'un observateur extérieur soit incapable de déterminer l'origine des fonds à la création d'une transaction PrivateSend »[24]. Par analogie, Dash indique que cette méthode confère aux fonds « les mêmes qualités d'anonymat que, par exemple, de l'argent liquide retiré à un distributeur »[25]. Cependant, contrairement à Monero, promoteur du « Privacy by Design », cette fonctionnalité reste optionnelle chez Dash et doit être sélectionnée par l'utilisateur.
3) ZCash (ZEC) fait usage de la technologie Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) qui permet de confirmer que l'expéditeur a suffisamment de Zcoin pour effectuer la transaction sans qu'il ne soit besoin de révéler les informations critiques afférentes à cette transaction[26] (adresses des parties et montant de la transaction). À l'instar de Dash, cette caractéristique de protection accrue de la confidentialité est optionnelle et doit être activée par l'utilisateur.

La question qui demeure est de savoir si ces techniques d'anonymisation seront considérées comme permettant de garantir des données juridiquement anonymes au sens du RGPD, comme il a été vu précédemment. Dans ce cas, le débat sur l'applicabilité du RGPD et du champ d'application de l'exception domestique aux transactions opérées au moyen de cryptomonnaies anonymes n'aurait plus vocation à être soulevé. Il appartiendra aux juridictions compétentes nationales et européennes d'en décider au cas par cas.

Si cette protection accrue en matière de confidentialité des données personnelles offerte par les cryptomonnaies anonymes semble en ligne avec l'esprit du RGPD, il reste que ce caractère anonyme est problématique au regard des exigences KYC/AML/CFT propres au secteur financier.

À cet égard, certaines dispositions ont été prises à l'effet d'empêcher ou à tout le moins limiter le recours aux cryptomonnaies anonymes. Ainsi, le Japon, au cours du printemps 2018, a annoncé l'interdiction de lister les cryptomonnaies anonymes, visant ainsi notamment Monero, Dash, Augur et ZCash[27]. En outre, en Corée du Sud, Korbit l'une des principales plateformes d'échange a supprimé de son listing ces mêmes cryptomonnaies anonymes[28].

En France, le rapport d'information de la Commission des finances de l'Assemblée nationale sur les monnaies

23. La Haute Cour du tribunal de commerce, 3 octobre 2017, *Data Protection Commissioner c. Facebook Ireland Limited, Maximilian Schrems*, 2016, n° 4809.P.

24. https://docs.dash.org/fr/stable/wallets/dashcore/privatesend-instantsend.html#dashcore-privatesend-instantsend.
25. *Ibid.*
26. P. de Filippi, A. Wright, *Blockchain and the Law, the Rule of Code*, Harvard University Press, 2018, p. 67.
27. https://www.newsbtc.com/2018/05/21/japans-coincheck-removes-monero-three-coins-fsa-ban/.
28. https://news.bitcoin.com/south-korean-crypto-exchange-korbit-xmr-zec-dash-rep-steem/.

virtuelles (janvier 2019) aborde brièvement ce sujet. Le président de la mission d'information dans son avant-propos attire l'attention du législateur sur ce sujet et regrette, en ces termes, l'absence de proposition d'interdiction : « de la diffusion et du commerce de crypto-actifs visant à garantir un anonymat complet en empêchant, par leur conception, toute procédure d'identification. C'est le cas d'un certain nombre de crypto-actifs (Monero, PIVX, DeepOnion, Zcash…) dont le but est de contourner toute possibilité d'identification des détenteurs. À ce jour, la régulation n'est pas allée jusque-là »[29].

L'anonymat, qui disqualifie la notion même de donnée personnelle, cristallise les inquiétudes en ce qu'il comporte le risque d'opacité des transactions et les conséquences afférentes en matière de blanchiment d'argent et de financement du terrorisme.

Notons à cet égard qu'en juin 2019, le Groupe d'Action Financière (GAFI) a énoncé les lignes directrices applicables aux transactions en cryptomonnaies[30]. Ces lignes directrices requièrent des plateformes d'échange qu'elles collectent les données d'identification de leurs clients (donneur d'ordre et bénéficiaire) étendant ainsi les exigences KYC/AML/CFT aux « *virtual asset service providers* » au même titre que les institutions financières traditionnelles.

Outre le traitement des données des clients par les plateformes dans le cadre des transactions en cryptomonnaies, les obligations compliance qui pèseront sur ces plateformes confirment le rôle de responsable de traitement leur incombant, lequel devra s'effectuer en conformité avec le RGPD.

Au vu de la sensibilité du sujet, le GAFI a tenu à clarifier son rôle s'agissant de la collecte des données et ainsi pu préciser :

> « *The updated FATF standards announced in June will require crypto-exchanges in all jurisdictions to identify their customers and keep that information securely and privately, so that it is available to law enforcement authorities when needed to investigate money laundering or terrorist financing. The same requirement already applies to banks and other financial institutions. The FATF does not collect customer data, and the FATF standards recognise the importance of privacy and data protection* »[31].

S'il est encore prématuré de se prononcer sur l'application pratique de ces dispositions au regard du RGPD, ces derniers développements confirment que la question de la protection des données personnelles constitue un point nodal des problématiques posées par les transactions en cryptomonnaies.

29. http://www.assemblee-nationale.fr/15/rap-info/i1624.asp#P801_232265.
30. https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.
31. https://www.coindesk.com/15-nations-plan-global-crypto-monitoring-system-under-fatf-report.