Lire cet article en ligne

La blockchain face au RGPD

La blockchain – ou « chaîne de blocs » en français – est une technologie sur laquelle peut s'appuyer un traitement de données à caractère personnel. Ses caractéristiques propres soulèvent de vraies difficultés pour la mise en œuvre des obligations prévues par le Règlement général sur la protection des données (RGPD).

Le 24 septembre 2018, la CNIL a publié une grille d'analyse et ses premières recommandations aux acteurs qui souhaitent y recourir lorsqu'ils mettent en œuvre un traitement de données personnelles.

La blockchain – ou « chaîne de blocs » en français – constitue un « *mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification* »[1].

Elle est notamment utilisée dans le domaine de la cybermonnaie, où elle remplit la fonction de registre public des transactions, comme par exemple le bitcoin, qui est toutefois loin d'être la seule monnaie virtuelle. Son utilisation peut s'appuyer sur les *smart contracts* (« contrats intelligents ») qui sont des programmes informatiques qui s'exécutent automatiquement : « si » le programme constate la réalisation d'une condition préprogrammée, « alors » il exécute les termes du contrat. Les *smart contracts* peuvent servir de support à une ICO (*initial coin offering*), qui est un mécanisme de financement de projet par émission de cybermonnaie ou jetons (*tokens*) sur une blockchain. Le projet de loi relatif à la croissance et la transformation des entreprises (PACTE) actuellement débattu en France prévoit d'ailleurs la création d'un cadre juridique d'une telle ICO.

Les identifiants, c'est-à-dire les clés[2], et les données inscrites sur la blockchain, dès lors qu'ils se rapportent à une personne physique identifiée ou identifiable, peuvent constituer des données à caractère personnelle.

Comment mettre en œuvre les règles du Règlement général sur la protection des données (RGPD) compte tenu des caractéristiques si singulières de la blockchain ?

Le 24 septembre 2018, la CNIL a publié une grille d'analyse et ses premières recommandations aux acteurs qui souhaitent y recourir lorsqu'ils mettent en œuvre un traitement de données personnelles[3].

Qui est le responsable de traitement ?

L'identification du responsable de traitement – défini comme celui qui détermine les finalités et les moyens de traitement de ces données – est cruciale. Les obligations prévues par le RGPD lui incombent principalement.

Pour la CNIL, la blockchain n'est pas un traitement en soi, mais une technologie. Toutes les personnes qui stockent ou déplacent des données ne sont en effet pas nécessairement des responsables de traitement.

Parmi ces personnes, la CNIL distingue les « accédants », qui ont un droit de lecture et d'obtention d'une copie de la chaîne, les « mineurs », qui valident une transaction et créent les blocs en appliquant les règles de la blockchain afin qu'ils soient « acceptés » par la communauté, et les « participants », qui ont un droit d'écriture (la création d'une transaction qu'ils soumettent à validation) et qui déterminent les finalités (les objectifs poursuivis par le traitement) et les moyens mis en œuvre (format de la donnée, recours à la technologie Blockchain, etc.).

Selon la CNIL, seul un participant pourrait être responsable de traitement :

- lorsqu'il est une personne physique et que le traitement est en lien avec une activité professionnelle ou commerciale ;
- lorsqu'il est une personne morale qui inscrit une donnée à caractère personnel.

Lorsqu'un groupe d'organismes décident de mettre en œuvre un traitement sur une blockchain pour une finalité commune, la CNIL recommande que les participants prennent une décision commune quant à la responsabilité de traitement 1) soit en créant une personne morale et en la désignant comme responsable de traitement ; 2) soit en désignant le participant qui prend les décisions pour le groupe comme responsable de traitement. À défaut, tous les participants sont susceptibles d'être regardés comme ayant une responsabilité conjointe.

Y a-t-il un sous-traitant ?

Dans certains cas, des personnes peuvent être qualifiées de sous-traitants. Or, la grande nouveauté du RGPD est d'imposer au sous-traitant le respect d'obligations.

Tel est par exemple le cas du développeur qui réalise le smart contract pour le compte du participant, responsable de traitement.

Les mineurs peuvent aussi être considérés comme des sous-traitants car ils exécutent les instructions du

responsable du traitement lorsqu'ils vérifient que la transaction respecte des critères techniques.

Ils devraient donc établir avec le participant, responsable du traitement, un contrat précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du RGPD.

Cette obligation de contractualiser les relations avec le responsable de traitement soulève cependant des difficultés lorsque la blockchain est publique (autrement dite ouverte : les protocoles de chaînes de blocs sont ouverts à l'écriture et à la lecture sans restriction), ce que la CNIL se contente de relever tout en encourageant les acteurs à avoir recours à des solutions innovantes.

Comment minimiser les risques ?

La minimisation passe avant tout par la limitation du recours à la blockchain aux seuls usages véritablement nécessaires. La protection de la vie privée dès la conception, Privacy by Design, oblige ainsi le responsable de traitement à réfléchir, en amont, à la pertinence du choix de cette technologie pour la mise en œuvre de son traitement.

Pour les transferts hors UE, et lorsque la blockchain est à permission, elle passe par l'utilisation des solutions existantes, telles que les règles d'entreprises contraignantes ou les clauses contractuelles types. Par contre, dans le cadre d'une blockchain publique, la CNIL reconnaît qu'il est très difficile pour le responsable de traitement de recourir à ces solutions.

La question de la conservation des données reste la plus problématique puisque l'une des caractéristiques de la blockchain réside dans le fait que les données qui y sont inscrites ne peuvent être techniquement modifiées ou supprimées : une fois que le bloc auquel est intégrée la transaction a été accepté par la majorité des participants, une transaction ne peut plus en pratique être modifiée.

La CNIL propose quelques pistes cependant pour « optimiser » la conservation des données.

Dans la mesure où les identifiants des participants, c'est-à-dire leurs clés publiques, sont essentiels au bon fonctionnement de la blockchain, la CNIL constate qu'il n'est pas possible de minimiser davantage les risques ; leur durée de conservation est alignée avec celle de la blockchain.

En ce qui concerne les données complémentaires stockées sur la blockchain, la CNIL recommande de privilégier les solutions dans lesquelles la donnée est traitée en dehors de la blockchain ou qu'elle soit enregistrée sur la blockchain par ordre de préférence :

- sous la forme d'un engagement cryptographique, ou
- sous la forme d'une empreinte de la donnée obtenue par une fonction de hachage à clé, ou, a minima,
- sous la forme d'un chiffré.

Si aucune de ces solutions ne peut être mise en œuvre, et lorsque cela est justifié par la finalité du traitement

et qu'une étude d'impact a démontré que les risques résiduels sont acceptables, les données peuvent être stockées soit avec une fonction de hachage sans clé soit, en l'absence d'autres possibilités, en clair.

Comment exercer les droits des personnes concernées ?

Pour la CNIL, le droit à l'information, le droit d'accès et le droit à la portabilité ne posent a priori pas de difficultés particulières.

S'il n'est pas techniquement pas possible de faire droit à une demande d'effacement, la CNIL constate que le choix du format de stockage de la donnée via un procédé cryptographique permet de s'en rapprocher : la suppression des données stockées en dehors de la blockchain et des éléments permettant la vérification permet de couper l'accessibilité à la preuve enregistrée sur la blockchain, en la rendant difficile voire impossible à recouvrer.

[1] Vocabulaire de l'informatique et de l'internet (liste de termes, expressions et définitions adoptés), JORF n°0121 du 23 mai 2017, texte n° 20

[2] La clé privée permet à l'utilisateur d'une blockchain d'initier une transaction en signant cryptographiquement son message, tandis que la clé publique sert d'adresse sur une blockchain (connue de tous, elle permet à un émetteur de désigner un destinataire).

[3] Disponible ici : https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles