La Blockchain face aux défis du RGPD

Juillet 2018

En quelques mots

Le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) est entré en vigueur, avec l'objectif ambitieux d'offrir à chaque citoyen de l'Union Européenne, un meilleur contrôle sur ses données à caractère personnel, tout en renforçant les obligations et sanctions pour les responsables de traitement.

Le RGPD ayant été élaboré dans un modèle prédominant où la collecte, le stockage et le traitement des données s'effectuent de manière centralisée par une entité *responsable de traitement* ou plusieurs entités en *co-responsabilité*, ces notions entrent en opposition avec le principe fondamental de décentralisation sur lequel repose la technologie DLT/Blockchain*.

Alors que la CNIL doit prochainement publier des lignes directrices concrètes pour tenter de concilier Blockchain et RGPD, Ailancy vous livre ses convictions sur les solutions à mettre en œuvre.

La DLT/Blockchain : des incompatibilités fondamentales avec le RGPD ?

L'IDENTIFICATION DU RESPONSABLE DE TRAITEMENT

Pour une entité traitant des données à caractère personnel de manière centralisée, le responsable de traitement généralement identifié est la personne morale (en tant qu'entité), représentée par le *Data Protection Officer* (DPO) qui agit comme garant de la conformité de l'entité vis-à-vis des tiers. En somme, le DPO est le « tiers de confiance », notamment pour permettre aux personnes concernées d'exercer aisément leurs droits, comme le RGPD le prévoit.

Dans un environnement DLT/Blockchain, l'identification du responsable de traitement apparaît plus complexe : elle dépend des politiques d'accès en place (*permissioned** ou *permissionless**), mais également des modes de gouvernance (privée*, publique* ou semi-publique), des modes d'accès (*webservices** ou *client**), du type de transactions et des données associées à celles-ci.

➢ ***Les principes de gouvernance de la Blockchain déterminent l'application des exigences du RGPD : par exemple, au sein d'une Blockchain publique, tout membre pourrait être considéré comme responsable de traitement.***

Gouvernance	Politique d'accès	Mode d'accès	Partage des responsabilités
DLT Privée	Permissioned	Interface / Web Services	**RT :** Entité opérant la DLT **ST :** N/A
		Interaction directe *(client)*	
	Permissionless	Interface / Web Services	
		Interaction directe (client)	
DLT Publique	Permissioned	Interface / Web Services	**RT :** Entité opérant le service web **ST :** Nœuds
	Permissionless		
	Permissioned	Interaction directe (client)	**RT :** Gestionnaire des habilitations **ST :** Nœuds
	Permissionless		**RT :** Utilisateur lui-même **ST :** Utilisateur lui-même

RT : Responsable de Traitement ; ST : Sous-Traitant

LA NOTION D'ACCOUNTABILITY

Le concept de reporting systématique auprès de l'autorité de contrôle (par le biais d'autorisations ou de normes simplifiées dans le cas de la CNIL) est remplacé par le paradigme de la responsabilité (*accountability*) des entités. Dès lors, charge incombe au responsable de traitement de documenter sa conformité selon les exigences du règlement (le registre des traitements en constitue un exemple notable).

Selon les paramètres de la DLT, le principe d'*accountability* du responsable de traitement s'oppose au principe d'*accountability* de la personne concernée. En effet, sur une DLT publique et *permissionless* et suivant le principe du *« sorry for your loss »*, chaque membre est réputé responsable de ses actes et doit lui-même protéger ses données à caractère personnel (y compris sensibles) en les cryptant et en les stockant *off-chain**, la représentation cryptographique de ses données étant sur la DLT.

➢ ***Chaque personne concernée pourrait, en toute connaissance de cause, être maître de ses propres données et de la manière dont celles-ci sont protégées et conservées : il s'agirait de l'avènement d'un nouveau paradigme d'accountability.***

LES ANALYSES D'IMPACTS RELATIVES À LA PROTECTION DES DONNÉES

Le RGPD consacre également la notion de *Data Privacy Impact Assessment* (DPIA) : tout traitement de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées

doit conduire à une analyse d'impact approfondie.

Désormais structuré en Comité Européen, le G29 avait défini, lors de la phase de mise en conformité, les critères permettant de déterminer les traitements devant faire l'objet de cette analyse d'impact : parmi eux, l'utilisation d'une nouvelle technologie, qui qualifiait systématiquement l'usage de la Blockchain, dans un traitement de données à caractère personnel, pour cette analyse complémentaire.

Complexe à mener, cette analyse requiert d'apprécier et d'évaluer l'ensemble des risques sur la vie privée des personnes concernées, au regard des mesures de sécurité mises en œuvre pour protéger les données. Cette analyse s'appuie donc fortement sur des modèles et des fonctions préexistantes de gestion et de maîtrise des risques.

- ***Il convient d'adapter, en amont, la méthodologie d'évaluation des risques de l'entité, afin d'y intégrer les risques propres à la technologie Blockchain (et notamment en termes de confidentialité des données qui y sont traitées et stockées).***

Quelles réponses à l'exercice de droits par les personnes concernées par le traitement ?

Préalablement, rappelons que le prérequis à l'exercice du droit est l'identification du responsable de traitement.

LE DROIT D'ACCÈS

Considérant que le droit d'accès est une notion instituée par la loi « Informatique et Libertés » de 1978, le processus de réponse à l'exercice de ce droit devrait être éprouvé au sein des entités réalisant un traitement centralisé des données.

Dans un environnement DLT/Blockchain et au-delà de la complexité à restituer les données à caractère personnel à la personne concernée, le RGPD exige du responsable de traitement qu'il fournisse des informations sur les éventuels transferts de données vers des entités basées en dehors de l'Union Européenne. Cette exigence suppose de connaître l'exhaustivité des *nœuds* (*nodes**) composant la Blockchain, mais également leur localisation.

Quand bien même le responsable de traitement pourrait effectuer ce recensement, chaque juridiction bénéficie d'une reconnaissance différente de la part de la CNIL.

- ***La mise en place d'un* Smart Contract *RGPD pourrait permettre l'extraction des données relatives à une personne, en vue d'être restituées. Néanmoins, la réponse ne pourrait être que partielle, compte tenu de la nature des informations qui doivent être fournies.***

LE DROIT À LA RECTIFICATION DES DONNÉES

Toute personne concernée « a le droit d'obtenir du responsable de traitement (…) la rectification des données à caractère personnel la concernant qui sont exactes ». Soulignons que l'exercice de ce droit est en dépendance directe avec la capacité à exercer son droit d'accès : il convient, en effet, que la personne concernée ait pu prendre connaissance des données erronées dont le responsable de traitement dispose à son égard.

- ***Aux limites précédemment évoquées, une alternative consisterait à générer une nouvelle transaction qui viendrait « annuler et remplacer » les données préexistantes, permettant de modifier l'état final de l'ensemble.***

LE DROIT À L'EFFACEMENT DES DONNÉES

Pour plusieurs motifs, toute personne concernée peut exercer son droit à l'effacement de ses données à caractère personnel : lorsqu'elles ne sont plus nécessaires aux finalités pour lesquelles elles ont été collectées, lorsque les données ont fait l'objet d'un traitement illicite ou lorsque la personne concernée retire son consentement, qui tenait lieu de fondement juridique au traitement.

Pour toute entité, le droit à l'effacement des données revêt deux enjeux majeurs :

- *L'archivage des données.* Avant l'effacement des données et afin de respecter les durées légales en vigueur, certaines données doivent être archivées en « base intermédiaire », ce qui suppose de restreindre l'accès à ces données. Un *chinese wall* doit être érigé, avec la création d'une politique de profils et d'habilitations.
- *La purge des données.* Au moment de l'effacement des données, il est nécessaire de distinguer, à un niveau *micro*, les données toujours nécessaires au(x) traitement(s) et celles pouvant effectivement être purgées. De fait, les évènements déclencheurs de l'effacement de chacune des données doivent être définis.

- ***L'exercice de ce droit est fortement dépendant de la gouvernance, des politiques d'accès et des modes d'accès. Avec un algorithme de consensus de type* Proof of Authority*, *dans une DLT privée / publique et* permissionless*, *l'effacement des données est possible sur simple accord des parties prenantes au système. Dans un environnement* Proof of Work* *ou* Proof of Stake**, *cela semble difficilement réalisable. La solution ultime étant de ne pas stocker ses données personnelles ou, à minima, de les hacher* / crypter* avant le stockage.***

LE DROIT À LA PORTABILITE DES DONNÉES

Ce nouveau droit permet à toute personne d'obtenir les données à caractère personnel qu'elle a fournies, ainsi que celles générées dans le cadre d'une activité de traitement.

Nombreuses sont les entités à rencontrer des difficultés dans la mise en œuvre opérationnelle de ce droit, car il pose la problématique, non de la compatibilité, mais de l'interopérabilité des systèmes, condition nécessaire pour répondre au double enjeu d'une transmission des données dans un format « couramment utilisé et lisible par machine » vers un autre responsable de traitement. La réponse à ces nouvelles exigences pourrait être la mise en place de méthodes standards et normées de partage de données (interfaces API, par exemple).

Dans un environnement DLT/Blockchain, ces difficultés semblent plus difficiles à surmonter : l'interopérabilité des protocoles est complexe et lourde à mettre en place. L'*atomic swap* (échange entre deux réseaux DLT/Blockchain) n'est pas une technologie suffisamment mature pour pouvoir être déployée à grande échelle.

La DLT/Blockchain, comme solution technique aux nouvelles exigences du régulateur ?

LE *DATA BREACH*

Au-delà des droits exerçables par tout individu, le RGPD renforce les obligations de chaque responsable de traitement en ce qui concerne la notification (auprès de l'autorité de contrôle et éventuellement, des personnes concernées) de toute violation de données à caractère personnel (ou *data breach*).

Face à des risques importants, tant au niveau financier (l'amende maximale s'élève à 20 M€ ou à 4% du chiffre d'affaires mondial, le montant le plus élevé étant retenu) qu'en termes de réputation et d'image, chaque entité a tout intérêt à mettre en place les mesures techniques et organisationnelles permettant de renforcer la sécurité des données à caractère personnel qu'elle est amenée à traiter, afin de limiter tout risque de *data breach*.

Dans un environnement DLT/Blockchain, si les attaques demeurent possibles, les mesures de sécurité restent intégrées *by default.*

- Une attaque *Sybil* où une personne ou entité contrôle plusieurs nœuds dans le but d'influencer le système de manière disproportionnée peut être limitée en basant la création de blocs sur la capacité de calcul ou le *stake* lié à la création de chaque nœud.
- Une attaque dite « des 51% », qui suppose que la personne ou l'entité dispose d'au moins 51% de la capacité de calcul ou du *stake* pour activer la « double dépense », peut être limitée par des mécanismes de type DPoS (*Delegated Proof of Stake*).

➢ ***Dans le cas d'une Blockchain publique, où nous avons précisé que chaque membre est lui-même responsable de la sécurisation de ses propres données, le principe de* data breach *ne pourrait s'appliquer.***

PRIVACY BY DESIGN* ET *PRIVACY BY DEFAULT

Dans l'objectif de renforcer la protection des données, les notions de *Privacy by Design* (c'est-à-dire, à la conception d'une nouvelle activité de traitement ou d'une nouvelle modalité de traitement des données) et de *Privacy by Default* sont fondamentales dans le cadre de l'entrée en vigueur du RGPD.

Sans négliger les risques qui lui sont inhérents, la technologie DLT/Blockchain assure néanmoins *by default*, un haut niveau de sécurisation des données, notamment par le principe des clés asymétriques.

➢ ***La technologie DLT/Blockchain semble donc être une réponse viable à ces nouvelles fortes exigences.***

En conclusion, la définition des principes de gouvernance de la Blockchain est cruciale.

Selon que la Blockchain soit privée, publique ou semi-publique, les exigences RGPD s'appliquent différemment. Une Blockchain publique ferait ainsi porter la responsabilité à chacun de ses membres.

Sur une Blockchain privée, de bonnes pratiques pourraient être mises en place : à titre d'exemple, ne pas stocker les données à caractère personnel sur la DLT, tout en gardant un lien entre le *haché* (*hashed*) et les données stockées en *off-chain*.

➢ ***Formaliser des règles de gestion pour concilier vos projets Blockchain aux exigences du RGPD, requiert d'associer à l'expertise règlementaire sur la protection des données, une connaissance fine des différents* frameworks *Blockchain. En outre, il est crucial de ne pas négliger la sensibilité des données qui seront traitées via la Blockchain, afin de mieux maîtriser l'ensemble des risques associés au déploiement de la technologie.***

Florian Hallant, Consultant
Florian intervient depuis 8 mois à la mise en conformité au RGPD d'un acteur bancaire et participe à la communauté Blockchain d'Ailancy.

Rachid Wakrim, Consultant
Rachid dispose d'une expertise DLT/Blockchain et API. Il participe aux actions de sensibilisation et d'exploration des différents cas d'usage.

GLOSSAIRE

Blockchain	Typologie de la DLT, groupant les transactions dans des blocs. La validation se faisant au niveau du bloc.
Client	Interface lignes de commande, la communication se faisant directement via le nœud.
Crypté	Output d'une fonction où le calcul de son inverse est possible sous condition de disposer de la clé privée.
Delegated Proof of Stake	Algorithme de consensus permettant de voter à des délégués suivant leurs avoirs et leur réputation au sein du réseau.
DLT	Tout type de registres digitaux utilisant des liens cryptographiques pour sécuriser les transactions.
Haché (*hashed*)	*Output* d'une fonction où le calcul de son inverse s'avère impossible.
Nœud (*node*)	Serveur hébergeant le programme permettant de valider les transactions / blocs sous différents algorithmes.
Off-chain	Transfert de valeur en dehors du registre.
Permissioned	Système soumis à l'adhésion avec des éventuels prérequis (ex : système d'échange de données KYC entre les banques).
Permissionless	Système libre d'accès (ex : bitcoin).
Privé	Système opéré par une seule entité (ex : Ripple).
Publique	Système opéré par plusieurs entités (ex : consortium).
Proof of Authority	Algorithme de consensus où chaque transaction requiert la validation de tout ou partie du réseau, suivant leur "autorité" dans le processus.
Proof of Stake (PoS)	Algorithme de consensus utilisant les avoirs en crypto pour la validation (preuve de transparence).
Proof of Work (PoW)	Algorithme de consensus utilisant la capacité de calcul pour la validation (preuve de travail).
Webservices	Interface graphique sur le web, la communication se basant sur les API.