Blockchain et RGPD, peut-on parler de conformité ?

Cette technologie de stockage et de transmission promet transparence et sécurité au travers d'un protocole constitué de blocks où des hébergeurs de données, appelés des mineurs, participent à authentifier la véracité d'informations cryptées en résolvant des calculs algorithmiques afin de valider chaque block de la chaîne.

En somme, lors d'une transaction entre deux personnes, chaque étape de la transaction est validée et hébergée par les mineurs, puis consignée dans un registre afin de débloquer la transaction finale. Ce système complexe vise ainsi à garantir la sécurité et la non-falsification de données.

Mais, lorsqu'on parle de sécurité de données, et surtout de données à caractère personnelles, peut-on parler de sécurité au regard du RGPD ? Y'a-t'il conformité ?

RGPD, de quoi parle-t-on ? Le Règlement Général sur la Protection des Données encadre le traitement des données personnelles sur le territoire de l'Union Européenne pour permettre aux citoyens de mieux contrôler le traitement de leurs données personnelles. Tout ou presque est une donnée personnelle, du prénom au numéro de compte bancaire. Ainsi, de la collecte au traitement, les entreprises et leurs soustraitants doivent garantir la protection de ces données.

Cette protection des données personnelles s'articule autour de cinq axes majeurs :

– les personnes concernées doivent être informées et donner leur accord à la collecte et au traitement de leurs données personnelles
– l'utilisation des données doit être transparente et pertinente au regard de leur collecte et de leur traitement
– les personnes concernées doivent avoir accès à leurs données de façon à pouvoir les consulter, les modifier et les supprimer à tout moment
– le partage et la circulation des données doit être encadré et limité, voire contractualisé – enfin, les données personnelles doivent être sécurisées tant sur le plan informatique que physique.

Mais alors, qu'en est-il de la sécurisation des données personnelles en blockchain ? Les utilisateurs de la blockchain peuvent-ils modifier et supprimer leurs données personnelles du registre quand ils le souhaitent ? Aussi, qu'en est-il des mineurs qui hébergent les données ?

Quand on parle de blockchain, il en existe deux types : blockchain publique et blockchain privée. La blockchain publique, ou ouverte, est consultable par tous et sans restriction quant à la participation au réseau. Tout le monde peut devenir membre du réseau d'une blockchain ouverte, il suffit de télécharger le protocole, la charte de fonctionnement du réseau, sans même avoir à dévoiler son identité.

Même si toute modification du protocole requiert un accord de la part des mineurs, les échanges au sein du réseau restent contrôlés en peer to peer. Autrement dit, il n'y a pas d'organe de contrôle prédéfini. Il n'y a donc aucune barrière d'entrée à ce réseau, ni aucun contrôle sur les transactions. Dans les faits, les mineurs sont libres d'héberger des données dans le pays qu'ils souhaitent.

En adoptant un point de vue RGPD, plusieurs étapes du protocole d'une blockchain publique manquent de conformité. On peut s'interroger sur plusieurs points. Tout d'abord concernant les données, car, même si les données sont cryptées au sein du réseau, elles n'en sont pas pour autant anonymes. Et en cas de transfert de données privées, difficile, voire impossible, de savoir exactement qui accède à ces données puisque le réseau est libre d'accès. Sans compter qu'une blockchain publique fonctionne sur un mode décentralisé, il devient encore plus difficile de suivre le parcours de ces données.

A la différence de la blockchain publique, dans une blockchain privée (ou fermée), les membres du réseau sont sélectionnés par une entité centrale, généralement le créateur du réseau, avant de pouvoir télécharger le protocole et donc de pouvoir utiliser les services du réseau. Non seulement la blockchain privée n'est pas décentralisée mais l'accès à son réseau est restreint par un organe de contrôle.

Question conformité on s'approche. Sauf que, pour être entièrement conforme, il faudrait pouvoir effacer des données personnelles sur demande. Autrement dit, effacer le registre, et les données hébergées par les mineurs. La CNIL est claire, en cas d'utilisations de données privées, la blockchain doit respecter les principes du RGPD. Alors appliquons la blockchain privée à un domaine sensible : la santé. Et plus particulièrement aux cas de transmission de dossiers électroniques de patients entre deux praticiens.

Qui dit blockchain privée dit qu'une entité centrale créée le réseau, élabore le protocole et restreint le téléchargement du protocole à des mineurs sélectionnés pour cette transmission. En théorie, cette blockchain permet de valider toutes les exigences du RGPD, sauf une. En effet, qu'arrive-t-il au dossier médical une fois la transmission effectuée ? Sachant que l'essence même d'une blockchain est de conserver les données afin d'en éviter la falsification, peut-on imaginer que toutes les parties prenantes effacent le dossier médical ?

Pourquoi pas. A condition que l'entité centrale devienne un réel organe de contrôle et définisse des règles strictes sur la conservation des données par les mineurs. Cette entité pourrait aussi imposer des serveurs dédiés à l'hébergement des données. L'entité centrale serait donc responsable de l'application du RGPD sur toute la blockchain.

Si par nature la blockchain n'est pas conforme au RGPD, elle n'y est pas incompatible pour autant. L'idée étant d'adapter la blockchain au type de prestation que l'on souhaite exécuter. Car s'il est aujourd'hui possible de se fier à une blockchain publique, basée sur un modèle collaboratif, pour garantir la traçabilité des produits alimentaires, il en est autre chose de s'en remettre uniquement à la collaboration de personnes tierces pour traiter des données personnelles.