ARTICLE

LE CEPD PUBLIE SES PREMIÈRES LIGNES DIRECTRICES SUR LE TRAITEMENT DES DONNÉES PERSONNELLES LIÉES À L'USAGE DE LA TECHNOLOGIE BLOCKCHAIN

IT et données personnelles | 06/05/25 | Florence Chafiol Benjamin Fontani

DATA PRIVACY

Le Comité européen de la protection des données (« **CEPD** ») a adopté, le 8 avril 2025, ses premières lignes directrices concernant le traitement des données à caractère personnel dans le cadre de l'utilisation de la technologie blockchain par les entreprises. Ces lignes directrices sont soumises à consultation publique jusqu'au 9 juin 2025.

Pour mémoire, la blockchain est une technologie de stockage et de transmission d'informations sans organe central de contrôle. Si la blockchain peut revêtir différents aspects techniques, sa nature traditionnellement décentralisée, immuable et transparente soulève des enjeux particuliers en matière de protection des données à caractère personnel. En particulier, un certain nombre de données à caractère personnel peuvent faire l'objet d'un traitement selon l'usage et la blockchain choisie.

S'il est évident que cette technologie pose un certain nombre d'interrogations quant à sa compatibilité et son articulation avec le règlement général sur la protection des données (« **RGPD** ») – l'exemple classique en la matière étant l'impact de l'immuabilité des données une fois enregistrées dans certaines blockchains[1] sur les droits à l'effacement ou à la rectification des personnes concernées – **le CEPD rappelle toutefois que l'impossibilité d'ordre technique ne peut être invoquée pour justifier le non-respect des exigences du RGPD**.

Les seize recommandations que le CEPD formule ont précisément vocation, en principe, à appréhender ces défis afin d'accompagner les entreprises dans leur utilisation conforme de cette technologie. Pourtant, le CEPD ne fournit que peu de réponses pratiques aux questions et difficultés soulevées, se bornant pour l'essentiel à rappeler les dispositions du RGPD.

Le CEPD met ainsi surtout en lumière les risques inhérents aux traitements de données à caractère personnel reposant sur cette technologie et décourage très fortement certaines pratiques, parmi lesquelles l'utilisation par défaut d'une blockchain publique *permissionless* ainsi que le stockage de données à caractère personnel « *on-chain* ».

Les difficultés liées à la qualification et la répartition de la responsabilité des acteurs de la blockchain

Un premier risque identifié par le CEPD réside dans la qualification et la répartition des responsabilités entre les différents acteurs intervenant au sein d'une blockchain. La nature décentralisée et la diversité des architectures complexifient l'analyse de la qualification au regard du RGPD, compte tenu de la multiplicité d'acteurs qui les composent. Il est néanmoins expressément rappelé dans les lignes directrices du CEPD que cette circonstance, et en général les difficultés techniques particulières du secteur, ne peuvent être invoquées pour justifier le non-respect du RGPD.

Or, l'identification du rôle respectif des parties, et leur qualité de responsable du traitement ou de sous-traitant, constitue une composante essentielle du régime de protection des données à caractère personnel. Le CEPD insiste ainsi sur l'importance d'évaluer avec soin la répartition de la responsabilité des acteurs dans le cadre des traitements effectués lors de l'utilisation de la blockchain.

Le CEPD précise que les nœuds[2] peuvent dans certaines circonstances, notamment dans les blockchains publiques, se voir reconnaitre la qualité de responsable du traitement et que les actions et responsabilités d'un nœud sont, le cas échéant, attribuées à la personne physique ou morale qui exploite ou contrôle le nœud. La confirmation de cette qualification de responsable de traitement doit ainsi être traitée avec la plus grande attention par les différents acteurs et notamment les mineurs, validateurs et les autres personnes gérant un nœud compte tenu des responsabilités qui en découlent.

Cette analyse des rôles des parties varie selon le modèle de gouvernance de la blockchain :

- **Dans les blockchains permissionnées,** une ou plusieurs entité(s) gère(nt) l'accès et les règles applicables à la validation et l'enregistrement des transactions. Ce modèle est, selon le CEPD, à privilégier dans la mesure où il permet une distribution plus lisible des rôles et donc une répartition plus aisée de la responsabilité, ce qui est un élément clé de la protection des droits et libertés des personnes.

En particulier, le CEPD précise que toute dérogation à cette gouvernance permissionnée ne devrait être envisagée qu'en présence de motifs particuliers, dûment étayés. Si tel est le cas et qu'une entreprise décide de déroger au modèle permissionné, cette dernière devrait également, selon le CEPD, se demander si l'utilisation de la blockchain est, de fait, réellement adéquate et évaluer s'il n'existe pas d'autres technologies susceptibles de répondre à ses besoins.

- **S'agissant des blockchains publiques *permissionless*** (*e.g.*, Bitcoin ou Ethereum), ouvertes à tous, entièrement décentralisées et ne nécessitant aucune autorisation ou tiers de confiance, le CEPD souligne que les nœuds peuvent, dans certains cas, être susceptibles de décider et/ou de modifier les finalités et/ou les moyens essentiels du traitement pour poursuivre leurs propres intérêts dans le cadre de leurs activités de minage ou de validation. Dans ce cas, le CEPD encourage expressément la création d'un consortium ou de toute autre forme d'entité juridique entre les nœuds. Cette entité, lorsqu'elle existe, serait alors responsable du traitement. Cette recommandation demeure pour l'heure largement théorique : l'hétérogénéité des intervenants et la difficulté, voire l'impossibilité pratique, de les identifier ou de les localiser font obstacle à sa mise en œuvre. Elle impliquerait en outre que des mineurs ou validateurs, souvent dépourvus de tout lien juridique entre eux, s'accordent spontanément pour assumer conjointement les obligations incombant aux responsables du traitement.

Par ailleurs, ces nœuds peuvent être situés en dehors de l'Union européenne. Dans ces circonstances, le CEPD souligne que l'utilisation d'une telle blockchain entraine des transferts de données en dehors de l'Union européenne, ce qui implique de se conformer à des exigences complémentaires visées au chapitre V du RGPD.

***Stockage de données à caractère personnel* on-chain**

Le CEPD alerte sur l'importance des risques pour la protection des données à caractère personnel lors de l'utilisation de la blockchain en tant que telle.

En effet, selon le CEPD, les blockchains sont susceptibles de contenir plusieurs catégories de données à caractère personnel. Le CEPD cite par exemple les identifiants de l'utilisateur ainsi que les autres métadonnées relatives aux transactions (horodatages, montants, fréquences) susceptibles d'identifier directement ou indirectement une personne physique. Le CEPD rappelle en outre que les données chiffrées ou hachées, dans le cadre d'un processus de pseudonymisation, sont toujours des données à caractère personnel.

Une fois stockées sur une blockchain, les données y seront conservées dans la plupart des cas sans qu'il soit possible, en pratique, de les supprimer ou de les modifier. Même s'il est techniquement possible de modifier les informations stockées au sein d'une blockchain, cela est très difficile à mettre en œuvre car cela nécessite que tous les nœuds mettent à jour leur copie de la chaîne (ou suppriment leur copie) et s'accordent sur la modification. Une telle action compromet les principes de cohérence et d'inviolabilité de la chaîne, qui sont au cœur de la raison d'être de la plupart des blockchains. Dans la pratique, une telle modification peut même ne pas avoir d'impact sur toutes les copies du bloc d'origine, ce qui signifie que les données d'origine sont immuables.

C'est dans ce contexte que **le CEPD recommande de ne pas, par principe, enregistrer de données à caractère personnel *on-chain*.** Les données en clair, chiffrées ou hachées devraient ainsi être stockées *off-chain*, avec des mesures de protection appropriées. En revanche, si l'enregistrement de données à caractère personnel sur une blockchain est nécessaire, le CEPD recommande l'utilisation de la preuve d'existence (*proof of existence*) sur la blockchain, renvoyant vers des données enregistrées *off-chain*.

Le CEPD reconnaît toutefois que dans certains cas limités, des données à caractère personnel peuvent être stockées dans une blockchain publique sous une forme permettant une identification directe, lorsque cela est justifié et strictement nécessaire eu égard à la finalité du traitement et si une analyse d'impact relative à la protection des données (« **AIPD** ») a été réalisée, concluant que les risques pour les personnes concernées ont été correctement pris en compte et atténués par des mesures appropriées.

Rappel de la nécessité de respecter les principes essentiels du RGPD

Le CEPD rappelle également que le responsable du traitement est tenu de s'assurer du respect des principes essentiels du RGPD résultant de l'article 5 de ce dernier, qui trouvent à s'appliquer indépendamment des difficultés techniques propres aux technologies qu'il choisit d'employer.

En premier lieu, il est rappelé que le choix de cette technologie parmi d'autres doit respecter le principe de nécessité prévu à l'article 5 du RGPD. Le responsable du traitement doit s'interroger sur la nécessité même de l'utilisation de la blockchain. En particulier, si les finalités poursuivies par ce dernier peuvent être atteintes en ayant recours à d'autres technologies offrant de meilleures garanties en matière de protection des données, alors le recours à la technologie blockchain doit être écarté. Il convient donc, le cas échéant, de documenter les raisons qui ont motivé le choix du recours à cette technologie.

Le respect des principes de minimisation et d'exactitude des données est par ailleurs un enjeu particulier face à la nature de la blockchain qui repose sur les ajouts successifs et irréversibles de données. Le CEPD se borne ici à rappeler que le respect de ces principes implique une obligation pour le responsable du traitement de démontrer que la technologie utilisée garantit que seules des données de qualité et strictement nécessaires au traitement sont utilisées, avec un niveau de confidentialité maximal.

S'agissant du principe de limitation de la durée de conservation, le CEPD estime que, dans les cas où le traitement ne nécessite pas une durée de conservation égale ou supérieure à la durée de vie de la blockchain, les données à caractère personnel ne devraient pas être enregistrées *on-chain*, sauf si cela est fait de manière à empêcher de manière effective l'identification des personnes concernées à l'issue du délai de conservation adéquat. En toute hypothèse, si la durée de conservation des données correspond à la durée de vie de la blockchain, le responsable du traitement doit être en mesure de justifier que cette durée de conservation est nécessaire et proportionnée au regard de la finalité du traitement.

La nécessaire réalisation d'une AIPD et la mise en œuvre du principe de privacy by design dans le cadre de l'utilisation d'une blockchain

Compte tenu du peu de marge de manœuvre dont le responsable du traitement dispose une fois que les données ont été enregistrées dans une blockchain, le CEPD souligne l'importance de l'analyse effectuée en amont et du soin apporté à la sélection initiale des données et des modalités de leur traitement.

En particulier, le CEPD insiste sur la nécessité d'effectuer une AIPD afin d'évaluer les risques pour les droits et libertés des personnes concernées et de permettre la mise en œuvre de mesures techniques et organisationnelles appropriées pour atténuer ces risques[3].

Par ailleurs, l'approche de la protection des données dès la conception et par défaut (*by design and by default*), apparait fondamentale, étant la seule à même de permettre l'implémentation de mesures techniques et organisationnelles réellement adéquates, destinées à assurer un niveau suffisant de protection des données pour les personnes concernées.

Le CEPD indique en outre que la facilitation de l'exercice des droits des personnes concernées doit également être prise en compte dès la conception du traitement. Dans la mesure où les données stockées sur la blockchain peuvent être difficiles à supprimer, le responsable du traitement devrait en effet tenir compte du respect de ces droits dès la phase de conception et veiller à ce que toutes les données à caractère personnel stockées puissent être rendues anonymes de manière effective en cas de demande d'effacement ou d'opposition. Cela suppose notamment que les données et métadonnées stockées *on-chain* ne permettent pas l'identification directe de la personne concernée et que toute donnée supplémentaire (*off-chain*) qui permettrait une identification indirecte, avec des moyens raisonnablement susceptibles d'être utilisés, soit effacée.

Compte tenu de la difficulté de mettre cela en œuvre en pratique, le CEPD recommande d'envisager d'autres outils si le recours à la blockchain ne s'avère pas nécessaire.

En conclusion, les lignes directrices du CEPD soulignent les difficultés et défis posés par l'articulation entre l'utilisation de la technologie blockchain par les entreprises et les impératifs du RGPD, qui imposent notamment une cartographie exhaustive des traitements, l'intégration du « *privacy by design* », la primauté des chaînes permissionnées et la règle « *off-chain first* ».

La position du CEPD, qui conditionne l'utilisation de la technologie blockchain à une AIPD robuste, fixe un seuil de conformité élevé aux acteurs concernés. En l'état de ces lignes directrices, le recours à une blockchain publique *permissionless* apparaît purement théorique, ne laissant que très peu de marge de manœuvre aux entreprises. Si la plupart des défis soulevés par le CEPD avaient déjà pu être identifiés par certains professionnels, ces lignes directrices offrent enfin des premières pistes de réflexion, avec une approche restrictive, dans un domaine qui, de toute évidence, continuera de susciter des questions d'application au regard du RGPD.

[1] Sur ce sujet, l'autorité de protection des données espagnole (AEPD) a publié en novembre 2024 une *technical note* intitulée *P roof of concept Blockchain and the right to erasure*

[2] Le CEPD définit un nœud comme « *des ordinateurs qui se connectent les uns aux autres et forment le réseau blockchain. Les nœuds peuvent aider à valider et à relayer les transactions. Ils peuvent être considérés comme des points individuels sur le réseau qui travaillent ensemble pour maintenir les propriétés de la blockchain.* »

[3] Sur les critères à prendre en compte dans le cadre d'une AIPD, cf. Les lignes directrices du Groupe de travail de l'article 29 concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, adoptées le 4 avril 2017 (WP 248 rév. 01)