Perspectives juridiques de l'émergence d'une identité décentralisée au service de droits numériques augmentés

Thibault Langlois-Berthelot

Perspectives juridiques de l'émergence d'une identité décentralisée au service de droits numériques augmentés

I/ La blockchain et l'identité décentralisée face au Règlement eIDAS

Un système d'identité numérique décentralisée permet aux personnes physiques de choisir les aspects de leurs identités qu'ils partagent avec des tiers tout en conservant une trace de ce partage. Cela est possible grâce à un registre décentralisé de données vérifiables, davantage connues sous son appellation anglophone de « blockchain technology ». Ce registre en principe décentralisé permet de relier en toute confiance des transactions de données (sous la forme de preuves cryptographiques) et diminue les risques d'impersonnalisation de l'identité de ses utilisateurs, sans pour autant révéler le contenu de leurs données à caractère personnel.

L'identité décentralisée change le paradigme et le rôle de la multitude des tiers interconnectés : les personnes physiques pourront désormais attester cryptographiquement de leurs différents titres et capacités juridiques, directement au sein de l'univers numérique. Cette nouvelle chaîne de confiance de l'identité numérique va au-delà d'une simple identification des personnes, dont les identités en ligne deviennent dynamiques et non plus statiques[1]. Le rôle des tiers de confiance (fournisseurs d'identité) nécessaire pour émettre et fournir une identité numérique est redéfini, en faveur de plus de transparence, d' accessibilité et de sécurité pour les personnes physiques.

De nombreux juristes s'accordent sur le fait que plusieurs textes encadrent suffisamment l'identité numérique grâce aux notions de données à caractère personnel[2], de respect de la vie privée[3] ou encore d'identification et d'authentification électronique. En effet, depuis le 23 juillet 2014, le Règlement n° 910/2014/UE *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*, plus communément nommé « Règlement eIDAS », propose une définition précise de l'identification électronique : « *processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale* »[4]. De même, l'authentification y est définie comme « *un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique* »[5]. Entré en vigueur le 17 septembre 2014, ce Règlement a pour ambition de construire un environnement interopérable pour les différents systèmes numériques mis en place au sein des États membres, afin de promouvoir le développement d'un marché dont le socle serait la confiance numérique. D'une part (i) ce Règlement permet d'établir des standards technologiques communs pour

[1] Concrètement, l'identité décentralisée sonne la fin des multiples identifiants et mots de passe aujourd'hui nécessaire pour se connecter à divers services en ligne : seules des preuves d'attributs d'identité (des attestations vérifiables - *VCs*) seront utilisées pour accéder à certains services ou permettre l'exercice de certains droits

[2] « […] *toute information se rapportant à une personne physique identifiée ou identifiable* », Règlement UE 2016/679 du 27 avril 2016, art. 4

[3] Art. 8 de la convention européenne des droits de l'homme (CEDH) entrée en vigueur le 3 septembre 1953 qui pose le fondement primordial du droit au respect de la vie privée et par extension celui indéterminé de l'identité des personnes : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.* »

[4] Art.3.1 du « Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE », OJ L, 2014, [consulté en ligne le 15 septembre 2021]

[5] Ibid.

évaluer la fiabilité des services numériques dits de « confiance »[6], et d'autre part (ii) il institue un pilier commun pour les services d'identification numérique des citoyens européens.

Si le Règlement eIDAS répond à une volonté renouvelée de créer une identité numérique européenne depuis plusieurs années[7], il est aujourd'hui en cours de révision[8] car confronté, entre autres[9], à plusieurs de ses limites depuis son entrée en vigueur. En effet, seulement 60% de la population de l'Union européenne, soit quatorze États membres, sont en mesure d'utiliser leurs systèmes d'identités numériques nationaux de manière transfrontalière. Les autres États membres ne disposent pas de *nœuds eIDAS*[10] dont les fonctions d'envoi sont pleinement opérationnelles. De plus, seuls 14 % des principaux prestataires de services publics dans l'ensemble des États membres autorisent l'authentification transfrontalière au moyen d'un système d'identité électronique.

Si cette première version du Règlement eIDAS, parfois surnommé « eIDAS-V1 », est toujours en vigueur, notons qu'elle a permis de répondre à certaines problématiques liées à la qualification juridique et à l'encadrement technique de l'identité numérique au sein de l'Union européenne. Dans une logique d'optimisation, sa récente proposition d'amendement par la Commission européenne[11] confère une nouvelle reconnaissance juridique aux technologies de registres et d'identité décentralisée. De ce fait, les attestations vérifiables[12] et la technologie blockchain[13] sont respectivement, implicitement et explicitement, évoquées dans cette même proposition. Parfois surnommé « eIDAS-V2 » par certains

---

[6] Le Règlement distingue cinq services de confiance (disposant chacun de deux ou trois niveaux de confiance sous-jacents) : (i) la signature pour les personnes physiques, (ii) les cachets électroniques pour les personnes morales, (iii) l'horodatage électronique et (iv) l'authentification en ligne de sites internet et enfin (v) les services d'envoi recommandé électronique

[7] « *Une identité électronique publique (eID) universellement acceptée est nécessaire pour que les consommateurs puissent accéder à leurs données et utiliser en toute sécurité les produits et services qu'ils souhaitent sans avoir à utiliser des plateformes non apparentées pour ce faire et à partager inutilement des données personnelles avec celles-ci* » *in* SHAPING EUROPE'S DIGITAL FUTURE, [consulté en ligne le 15 septembre 2021], doi:10.2759/091014, pages 6 sur 9

[8] Il est fait référence au lancement d'un processus de consultation en juillet 2020 puis au projet de proposition de Règlement modificatif publié en juin 2021. La version finale du texte « *eIDAS-V2* » devrait être publiée et adoptée au deuxième trimestre 2022

[9] S. COUTOR, C. HENNEBERT, M. FAHER, Restitution des ateliers du groupe de travail « blockchain et identité » (BCID), Octobre 2020, Ministère de l'Intérieur, [consulté en ligne le 04/10/2021] : « […] *le cadre eIDAS est trop limité pour intégrer la blockchain. Destiné à encadrer la fourniture d'un ensemble d'attributs déterminés (l'ensemble minimum d'attributs obligatoires qui identifient la personne, ou « identité pivot ») définis dans l'acte d'exécution 2015/1501, eIDAS ne permet : (i) ni la minimisation des données et la divulgation sélective d'attributs, (ii) ni l'utilisation de références anonymisées comme par exemple les assertions vérifiables certifiées (Verifiable Credentials [VCs]) basées sur le modèle de données du W3C, (iii) ni la communication d'attributs connexes d'identification, autres que les « données pivot » (qui, renvoyant à l'identité juridique, servent à identifier la personne), (iv) ni des services en ligne offerts par le privé, (le Règlement traite uniquement de l'action des administrations publiques), (v) ni l'hébergement des données personnelles sur un dispositif personnel mobile de façon sécurisée.* », page 83 sur 102

[10] Ces *nœuds* représentent des serveurs standardisés qui fonctionnent avec un protocole commun maintenu par le bras droit technique de la Commission européenne : le « *Connecting Europe Facility* »

[11] Op. Cit

[12] L'amendement désigne les attestations vérifiables en tant que « attestation électronique qualifiée d'attributs » ou « *qualified electronic attestation of attributes* » en anglais. Ainsi, une *attestation électronique qualifiée d'attribut* est une « *attestation électronique d'attributs délivrée par un prestataire de services de confiance qualifié* », Op. Cit *in* (45)

[13] L'amendement ne nomme ni ne cite la technologie blockchain, mais préfère le terme « *Electronic Ledger* » dans un souci de neutralité technologique. Si cette ambivalence peut faire référence à tous types de registres électroniques qu'ils soient centralisés, décentralisés ou bien hybrides, il convient d'admettre que la volonté du législateur européen est de permettre une qualification puis une reconnaissance juridique aux technologies blockchains en les incluant dans cette large définition

juristes spécialisés, son objectif est de passer de 60% d'utilisation actuelle des identités numériques nationales mises en place par « eIDAS-V1 », à 80%[14]. Cet objectif est d'autant plus ambitieux qu'il fait face à un temps d'application très court, d'environ trois ans.

Les points cardinaux d'eIDAS-V2 peuvent se résumer comme suit :

- Elle propose l'ajout de trois nouvelles catégories de services de confiance (en complément de ceux détaillés en note de bas de page n°6) : les services d'archivage électronique[15], la gestion des dispositifs de création de signatures électroniques à distance[16], les registres électroniques (y compris blockchain)[17] et enfin les attestations électroniques d'attributs (*VCs*)[18].

- Une présomption de fiabilité et d'authenticité est conférée aux registres électroniques dits qualifiés : « *Un registre électronique qualifié bénéficie de la présomption de l'unicité et de l'authenticité des données qu'il contient, de l'exactitude de leur date et de leur heure, et de leur ordre chronologique séquentiel au sein du grand livre.* »[19]. Les conditions pour qu'un registre électronique soit considéré comme qualifié sont telles que : (i) ledit registre est créé par un ou plusieurs prestataires de services de confiance qualifiés, (ii) il garantit l'unicité, l'authenticité et l'ordre correct des entrées de données enregistrées, (iii) il assure l'ordre chronologique séquentiel et l'exactitude de la date et de l'heure correcte des données, (iv) il enregistre les données de manière à ce que toute modification ultérieure des données soit immédiatement détectable.

- Concernant l'identification électronique (soit l'identité numérique), de nouveaux portefeuilles numériques nommés « European Digital Identity Wallets - EIDWs » ou « mallettes d'identité numériques », devront être proposés puis mis en place par les États membres d'ici 2024 (cette obligation leur incombe).

    - Plus précisément, ces EDIWs seront mis à la disposition des citoyens, des résidents et des entreprises de l'Union européenne qui souhaitent s'identifier ou fournir la confirmation de certaines informations personnelles[20]. Ils pourront être utilisés pour accéder à des services en ligne et hors-ligne, publics et privés, et de façon transfrontalière et non limitative dans tous les États membres de l'UE.

---

[14] « […] *by 2030, all key public services should be available online […] and 80% citizens should use an eID solution.* » *in Commission proposes a trusted and secure Digital Identity for all Europeans*, [consulté en ligne le 3 juin 2021]

[15] « *Electronic archiving services* », Section 10, art.45g

[16] « *Management of remote electronic signature creation devices* », (28), art. 29a

[17] « *Electronic Ledgers* », Section 11 & (34) : « *Un registre électronique combine l'effet de l'horodatage des données avec la certitude de leur origine, comme la signature électronique, et présente l'avantage de permettre des modèles de gouvernance plus décentralisés, adaptés aux coopérations multipartites. [...]. Il fournit la base de solutions avancées pour l'identité auto souveraine (SSI) et favorise des services publics plus efficaces et transformateurs.* »

[18] « *Electronic attestations of attributes* », Section 9

[19] Op. Cit, art. 45h

[20] Ces *mallettes d'identité* devront « *permettre aux utilisateurs de stocker des données d'identité, des justificatifs et des attributs pour les fournir sur demande aux parties qui se fient à eux et les utiliser pour l'authentification en ligne et hors ligne et pour créer des signatures et des sceaux électroniques* », (i) (42)

- La responsabilité de ces mallettes d'identités incomberait aux États membres[21] et leurs certifications ne seront pas soumises à des processus « *d'examen par les pairs* »[22] comme l'exige actuellement eIDAS-V1. Un État membre devra fournir une interface commune aux utilisateurs et citoyens afin de permettre une interaction facilitée avec le portefeuille d'identité numérique européen. À cette fin, une « *Marque de confiance du portefeuille d'identité numérique européen* » ou « *Trust Mark* »[23] sera mis en place. Un EDIW doit ainsi être reconnu et accepté comme une alternative à l'authentification forte du client (« *Strong Customer Authentication – SCA* »)[24].

- En matière de protection des données personnelles, l'utilisation des données doit tout d'abord être sous le contrôle de l'utilisateur et doit lui permettre une « *divulgation sélective* » de ses attributs d'identité[25]. L'émetteur d'un EDIW ne peut pas collecter d'informations personnelles[26] et doit pouvoir assurer une « *identification unique* » des utilisateurs[27]. Une combinaison par défaut limitée des données personnelles doit être effectuée : l'émetteur du portefeuille d'identité ne pourra pas combiner les données d'identification avec des données personnelles provenant d'autres services (excepté si l'utilisateur en fait la demande). Finalement, une séparation logicielle et physique des données personnelles par rapport à tout autre type de données devra en principe être appliquée.

- Un État membre devra fournir un EDIW qui s'imposera aux « *très grandes plateformes en ligne* »[28] tout en étant gratuit et d'utilisation facultative pour les citoyens européens. Parallèlement, une combinaison restreinte des données à caractère personnel des utilisateurs devra être assurée : l'émetteur d'un portefeuille ne pourra pas combiner des données d'identification avec des données personnelles provenant d'autres services (excepté si l'utilisateur en fait la demande). De façon complémentaire et concernant les fournisseurs de périphériques matériels (opérateurs mobiles, etc.), cette séparation

---

[21] Les EDIWs doivent être « délivrés » ou « approuvés » par les autres États membres, ce qui a des implications en termes de responsabilité : un État peut ainsi être tenu responsable en cas de violation des données à caractère personnel, art.10a

[22] Possibilité de s'appuyer sur la certification pour garantir la conformité au Règlement en remplacement du processus d'examen par les pairs : les EDIWs seront évalués par référence à des « *normes et références techniques communes* » et seront donc reconnus de façon égale au sein de l'Union européenne. En vertu de l'art. 42 du RGPD

[23] Section 1, 4.(a).(4)

[24] *« EDIW […] provide a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestation of attributes »*, Section 1, 4.(a).(4).(d)

[25] Op. Cit 3. *In « RESULTS OF EX-POST EVALUATIONS AND IMPACT ASSESSMENTS »* : « […] *permettant aux utilisateurs de choisir quand et avec quel fournisseur de services privé partager divers attributs, en fonction du cas d'utilisation et de la sécurité requise pour la transaction concernée.* » ; (29) « *L'EDIW devrait permettre techniquement la divulgation sélective d'attributs aux parties concernées.* »

[26] En principe, il ne doit pas s'opérer de collecte des données d'utilisation pour ces portefeuilles d'identité : l'émetteur d'un portefeuille ne peut pas collecter les données d'utilisation sauf si elles sont strictement identifiées comme nécessaires au fonctionnement du portefeuille

[27] Op. Cit, art 11a

[28] Les grandes plateformes comme Amazon, Google ou Facebook seront également tenues d'accepter l'utilisation des portefeuilles d'identité numérique de l'UE à la demande de l'utilisateur, par exemple pour prouver son âge

logicielle devra s'accompagner d'une séparation physique des données personnelles grâce à un composant sécurisé ou « *secure element* ».

- À l'heure actuelle, si certains principes d'eIDAS-V2 sont formels et inédits, la généralité de certaines définitions peut laisser place à une certaine ambiguïté d'interprétation, notamment pour les États membres et les fournisseurs d'identité. Dès lors, de nouvelles modifications dudit texte devraient en principe intervenir avant son adoption courant 2023. Si avec certitude l'identité numérique européenne est en marche, de nombreux éléments et détails de techniques et juridiques de cette identité numérique d'un nouveau genre sont à préciser et décider.

- En définitive, comme le souligne eIDAS-V2 : « *un processus de coopération étroite et structurée entre la Commission, les États membres et le secteur privé est nécessaire.* »[29]. Pour cela, une « Boîte à outils » ou « Toolbox » permettra de mettre en place une architecture technique qui repose sur des standards et des pratiques communes que les États membres devront respecter à propos de leurs solutions : (i) permettre la fourniture et l'échange d'attributs d'identité, (ii) assurer la fonctionnalité et la sécurité des EDIWs, (iii) ériger une gouvernance pour les EDIWs ou encore étudier leurs dépendances à l'égard des fournisseurs d'attributs et d'identité. La Commission européenne envisage aussi de mettre en place des « Codes de conduite autorégulateurs »[30] pour faciliter la mise à disposition et l'utilisation des EDIWs. Cette boîte à outils devrait être implémentée en septembre 2022.

Par conséquent, si cette proposition est adoptée, un service en ligne (public ou privé[31]) qui recourt à la technologie blockchain pourra être accessible à travers toute l'Union européenne, dès lors qu'il répond aux exigences du Règlement eIDAS (V1 & V2). Ainsi, une solution d'identité décentralisée déployée par un État membre se verra attribuer l'un des trois niveaux de confiance initialement institués par eIDAS[32].

II/ La blockchain et l'identité décentralisée face au RGPD

De manière intuitive, la technologie blockchain semble avoir pour vocation de libérer les personnes du principe d'autorité. Cependant, le 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 (RGPD)*[33], exige que les responsabilités soient désignées en matière de gestion des données à caractère personnel.

---

[29] Op. Cit (36)

[30] (28) « *Des codes de conduite d'autorégulation au niveau de l'Union ("codes de conduite") devraient être élaborés afin de contribuer à une large disponibilité et à une grande facilité d'utilisation des moyens d'identification électronique, y compris les portefeuilles d'identité numérique européens, dans le cadre du présent Règlement. Les codes de conduite devraient faciliter une large acceptation des moyens d'identification électronique, y compris les EDIWs. Ils devraient être élaborés dans les douze mois suivants l'adoption du présent Règlement.* »

[31] Et non plus simplement public comme dans la version actuellement en vigueur du Règlement eIDAS (V1), qui limite les services d'identification électronique aux services publics

[32] Trois niveaux d'assurance sont spécifiés pour les identités électroniques dans le cadre d'eIDAS, qui font référence au degré de confiance dans l'identité revendiquée d'une personne. Ces niveaux comprennent des critères détaillés permettant aux États membres de comparer leurs moyens d'identification électronique à un point de référence (*faible*, *substantiel* et *élevé*). Les mises en œuvre actuelles de l'identité décentralisée ont pour objectif d'être reconnues avec un niveau d'assurance spécifié comme à minima substantiel et si possible élevé

[33] Op. Cit : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

Parce qu'une blockchain ne semble être qu'un protocole dénué de tout intermédiaire et donc de tout responsable de traitement, le RGPD semble prime abord incompatible avec cette technologie[34]. En réalité, la blockchain est une infrastructure informatique qui impose le recours au pseudo anonymat et aux algorithmes de chiffrement par défaut. Ainsi, la sécurité et la confidentialité des données horodatées sur une blockchain ne sont pas remises en cause et incompatibles avec ses principes fondateurs de transparence et de libre accès (car l'intégrité des données est assurée par des mécanismes de signature et d'horodatage numériques).

Toutefois, si l'utilisation de mécanismes algorithmiques et cryptographiques de gestion des clés publiques et privées, pour signer ou horodater des jeux authentiques de données, est en principe inhérente à une blockchain, il n'en demeure pas moins que des données personnelles peuvent faire l'objet d'un traitement informatique en son sein. Dès lors, ces outils qui favorisent le pseudo anonymat ne sont pas infaillibles selon les cas d'usage et ils peuvent permettre d'identifier directement ou indirectement une personne physique. Ainsi, l'application des grands principes et des exigences édictés par le RGPD est incontournable : droit à l'effacement[35], portabilité[36] et transparence[37] des données, durée limitée de conservation des données[38], consentement des personnes physiques[39], droit de rectification[40], responsabilité du responsable de traitement[41], droit à l'information[42], entre autres.

Fondamentalement, la CNIL recommande un strict respect du principe de *minimisation* des données[43], y compris par l'utilisation non optimale « *d'engagement cryptographique* »[44]. Si ces méthodes de pseudo anonymisation cryptographiques des données personnelles ne sont pas possibles à mettre en œuvre dans un premier temps, une étude d'impact doit être réalisée. Si les risques sont acceptables, les données peuvent être stockées avec des mécanismes cartographiques faibles ou bien directement en clair au sein de ladite blockchain.

En matière d'identification des responsables de traitement des données personnelles, elle énonce que les acteurs qui possèdent « *un droit d'écriture sur la chaîne et qui décident de soumettre une donnée à la validation des mineurs peut être considérés comme responsables de traitement* »[45], en précisant qu'un acteur est une partie prenante responsable de traitement dès lors qu'elle « *détermine les finalités (les objectifs poursuivis par le traitement) et les moyens mis en œuvre (format de la donnée, recours à la technologie Blockchain, etc.)* »[46].

---

[34] « *[…] le modèle décentralisé de gouvernance des données de la technologie Blockchain et la multiplicité des acteurs intervenant dans le traitement de la donnée complexifient la définition des rôles de chacun.* » *in Premiers éléments d'analyse de la CNIL – Blockchain*, publié en septembre 2018, consulté en ligne le 04/10/2021, page 2 sur 11

[35] Art. 17 du RGPD

[36] Op. Cit, art. 20

[37] Op. Cit, art 12

[38] Op. Cit, art 5

[39] Op. Cit, art 7

[40] Op. Cit, art 16

[41] Op. Cit, art 24

[42] Op. Cit, art 13

[43] « *Le principe de minimisation prévoit que les données à caractère personnel doivent être (i) adéquates, (ii) pertinentes et (iii) limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* »

[44] Il s'agit « *d'un mécanisme qui permet de figer une donnée de telle sorte qu'il soit possible, avec des éléments supplémentaires, de prouver ce qui a été figé, et à la fois impossible de la retrouver ou de la reconnaître à partir de cette seule version 'engagée'* », Op. Cit, page 8 sur 11

[45] Op. Cit *Premiers éléments d'analyse de la CNIL – Blockchain*

[46] Ibid.

Selon qu'il s'agisse d'une blockchain publique, privée ou hybride[47], les droits des personnes ci-avant cités ne s'appliqueront pas de façon systématique, ni linéaires. Selon la CNIL : « *Il convient de privilégier une Blockchain à permission [blockchain hybride] qui permet d'avoir une meilleure maîtrise sur la gouvernance de la donnée personnelle, s'agissant notamment des transferts hors UE.* » car « *les règles d'entreprises contraignantes ou les clauses contractuelles types, sont entièrement applicables dans la Blockchain à permission.* ». Cependant, la CNIL précise qu'une « *vigilance particulière devrait être portée sur les mesures mises en œuvre pour assurer la confidentialité de la Blockchain si celle-ci n'est pas publique.* »[48].

Concernant l'identité décentralisée, l'utilisation d'identifiants numériques ou « *identifiants numériques décentralisés - DIDs* »[49] est une nécessité technique. La CNIL « *considère qu'il n'est pas possible de les minimiser davantage [les identifiants numériques] et que leurs durées de conservation sont, par essence, alignées sur celles de la durée de vie de la Blockchain.* »[50]. Par conséquent, les *DIDs* représentent non seulement des mécanismes *d'engagement cryptographique* au sens de la CNIL, mais entrent également et surtout en conformité avec le principe de *minimisation* des identifiants numériques sur blockchain sur lesquels la CNIL a statué en 2018.

Par contiguïté à la technologie blockchain et à l'identité décentralisée, les « automates exécuteurs de clauses - AEC »[51] ou « Smart contract » peuvent aussi entrer en considération dans l'élaboration d'une solution d'identité décentralisée. En principe, les « *mesures appropriées* »[52] évoquées par la CNIL pour garantir la disponibilité d'une telle solution hybride (blockchain, *VCs, DIDs*)[53] implique une certaine difficulté de mise en œuvre : un utilisateur devrait pouvoir obtenir une intervention humaine, exprimer son point de vue ou contester la décision après l'exécution d'un AEC. Il convient donc que le responsable de traitement prévoit la possibilité d'une intervention humaine qui permette de remettre en cause la transaction effectuée en accordant à la personne concernée le droit de contester ladite transaction : « *même si le contrat a déjà été exécuté, et ceci indépendamment de ce qui est inscrit dans la blockchain* »[54]. Dans les faits, si cela est techniquement possible à mettre en place pour les blockchains privées et hybrides, de telles fonctionnalités s'avèrent compliquées à assurer pour les blockchains publiques.

En conclusion, la technologie blockchain et le RGPD ne sont pas en principe – dans leur technique

---

[47] Dans une *blockchain publique*, tous les utilisateurs peuvent envoyer et recevoir des transactions, voir son historique, ainsi que participer à la mise à jour de ladite blockchain (protocole, minage, nœuds, etc.). Dans le cas où certaines limitations partielles ou totales sont appliquées pour l'autorisation des utilisateurs, on parle de blockchain *hybride*/*consortium* (protocole partiellement bridé par quelques entités) ou *privée* (protocole totalement bridé par une entité). Dans ces deux derniers cas, le système blockchain n'est plus entièrement décentralisé

[48] Op. Cit, page 7 sur 11

[49] La « *Decentralized Identity Foundation* » définit les standards techniques des « *decentralized identifiers – DIDs* »

[50] Op. Cit, page 7 sur 11

[51] Le terme « *d'automates exécuteurs de clauses* » est introduit par la Commission d'enrichissement de la langue française en janvier 2021. Vocabulaire des actifs numériques (Texte 108 sur 142). Journal officiel de la République française. Pour plus d'informations pour comprendre les *smart contracts* confère les sous-parties dédiées à ce sujet dans ce livre

[52] Art. 32 du RGPD : « *[…] le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris selon les besoins : […] des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;* »

[53] Confère aux sous-parties afférentes de ce livre pour une bonne compréhension de ces concepts

[54] Op. Cit, *Premiers éléments d'analyse de la CNIL – Blockchain*, consulté en ligne, page 10 sur 11

respectivement informatique et juridique – incompatibles, comme le soulignent à juste titre certains juristes[55]. En réalité, la blockchain permet de mettre en place une nouvelle gouvernance sur les données qui est optimisée[56] : elle s'avère complémentaire avec une majorité des grands principes du RGPD, dès lors qu'une considération préalable est accordée à celui-ci puis appliquée aux projets recourant à la technologie blockchain et/ou aux solutions d'identités décentralisées.

Conclusion

Les choix technologiques évoqués pour nos futures identités numériques s'imposeront par les usages du marché et non par coercition du législateur européen, qui recherche avant tout une neutralité technologique tout aussi évidente qu'essentielle pour garantir des solutions d'identification électroniques démocratiques et durables. Dans les faits, chaque État membre décidera de l'implémentation technique, centralisée ou bien décentralisée, de cette future identité numérique européenne.

Néanmoins, force est de constater que les avantages techniques d'une identité et d'un registre décentralisé ont su séduire le législateur européen tant au regard de l'applicabilité renforcé du RGPD qu'ils permettent, qu'au regard de la nouvelle proposition d'amendement du Règlement eIDAS qui cherche à débloquer les derniers verrous juridiques auxquels il est confronté. Cette volonté du législateur européen ne peut s'interpréter que sous réserve que les textes (eIDAS & RGPD), fondamentaux pour nos droits en ligne, soient pleinement respectés par les acteurs du marché européen de l'identité numérique.

Pour conclure, l'identité numérique décentralisée vient diluer la complexité probatoire de nos attributs d'identité qui évoluent au sein de l'espace numérique. Grâce aux attestations vérifiables (*VCs*) et à la technologie blockchain, la preuve des droits numériques d'une personne est simplifiée, renforcée et fiabilisée par de nouveaux schémas et mécanismes cryptographiques. Cette présomption de fiabilité des *VCs* et des *DIDs* - bien qu'elle ne soit pas encore reconnue aujourd'hui[57] - se couple à une réduction drastique des frictions entre les services en ligne et l'identité numérique des utilisateurs, qui ne s'effectue plus au détriment de leurs données personnelles.

***

[55] Maître Jérôme Deroulez explique qu'en : « *dépit d'un mode de fonctionnement parfois antinomique avec les principes du droit à la protection des données, la blockchain apportera peut-être paradoxalement les solutions techniques les plus à même de protéger ces données à l'ère du numérique et de garantir l'effectivité d'un droit parfois mis à mal dans un environnement technologique de plus en plus complexe et transnational* », propos issus de *Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies*, [consulté en ligne le 05/10/2021]

[56] « *Outre la minimisation des risques pour la personne, vue précédemment, le format choisi pour inscrire la donnée sur une Blockchain peut permettre de faciliter l'exercice des droits des personnes.* », Op. Cit, *Premiers éléments d'analyse de la CNIL – Blockchain*

[57] L'adoption de la proposition d'amendement du Règlement eIDAS permettra de faire reconnaître, par transposition en droit interne, cette présomption de fiabilité des attestations vérifiables ainsi que de l'historique des transactions d'un registre électronique décentralisé