Blockchain et droit à l'oubli

Primavera de Filippi, Michel Reymond

Blockchain et droit à l'oubli

Primavera De Filippi, CERSA/CNRS & Berkman-Klein Center at Harvard
Michel Reymond, University of Geneva

I. Intro

Le 13 mai 2014, la Cour de Justice de l'Union Européenne (CJUE) rendait l'arrêt Google Spain, qui accordait aux citoyens européens le droit de demander l'effacement des résultats de recherches menant à des sites internet contenant des informations inexactes, inadéquates ou excessives les concernant. Le droit à l'oubli repose–sur la protection de la vie privée : il implique/postule que les personnes physiques n'ont pas à rendre indéfiniment des comptes sur les événements honteux ou désagréables auxquels ils ont été associés dans un lointain passé. De façon plus large, on pourrait décrire le droit à l'oubli comme une tentative de conciliation entre, d'une part, le besoin humain d'être réhabilité.e ou pardonné.e, et, d'autre part, le rôle d'Internet en tant que registre numérique de l'histoire (Leta Jones, 2016)

Cette opposition est d'autant plus forte depuis l'apparition de nouvelles bases de données décentralisées, connues sous le nom de blockchains; soit, la technologie utilisée par le réseau Bitcoin. Dans la mesure où la blockchain est inaltérable et résistante à la censure et à la modification par conception/dans sa conception, elle entre en conflit direct avec le droit à l'oubli. La présente contribution cherche à analyser les défis posés par ces technologies émergentes vis-à-vis du droit à l'oubli. Nous présenterons d'abord le droit à l'oubli (I) et la blockchain (II), nous analyserons ensuite si le droit à l'oubli a titre à s'appliquer à la blockchain (III) et, si tel est le cas, nous examinerons plus en avant si et comment les obligations afférant au droit à l'oubli peuvent être exécutées sur la blockchain. (IV).

II. Définitions

II. A. Le droit à l'oubli

Le droit à l'oubli est une obligation de droit communautaire de la protection des données, imposée aux moteurs de recherche. Il permet aux citoyens européens de demander le retrait de résultats de recherches liés à leur nom et qui mèneraient à des sites internet contenant des informations "inexactes, inadéquates ou excessives", et qui ainsi porteraient atteinte à leur vie privée. Le droit à l'oubli a été déduit par la CJUE du droit Européen de la protection des données, et notamment de la Directive 95/46/CE, dans l'arrêt Google Spain, en Mai 2014. A l'issue de celui-ci, un ressortissant espagnol a pu amener le moteur de recherche Google à retirer un lien, apparaissant suite à une recherche portant son nom, vers une notice

originellement publiée en 1998 et archivée sur le site d'un journal espagnol; celle-ci portait sur sa participation à une vente aux enchères dans le but de recouvrer ses dettes de sécurité sociale (CJUE, 2014). L'obligation concerne tous les moteurs de recherche, mais la position hégémonique de Google sur ce marché en a fait le principal destinataire. La société a par conséquent mis en place un processus décisionnel interne pour le déréférencement et a reçu jusqu'à présent environ 500 000 requêtes, conduisant au retrait d'environ 1 500 000 résultats au total.

Il faut noter que le droit à l'oubli ne s'applique qu'aux liens fournis par un moteur de recherche non-spécifique à la suite de la recherche du nom d'une personne (CJE, 2014, at par. 96). *A contrario*, il n'affecte pas directement l'intégrité du contenu référencé, comme par exemple le site web d'un journal, un article ou un billet émis sur un blog; il n'a pas non plus vocation à s'appliquer aux résultats obtenus en cherchant des mots-clefs autres que nom et prénom. Ainsi, le droit à l'oubli est conceptuellement plus proche d'un droit limité au déréférencement ~~partiel~~ plutôt qu'à un droit d'être oublié au sens littéral. Et même s'il n'est pas exclu que ce droit puisse éventuellement s'appliquer au-delà des simples moteurs de recherche généralistes, et donc s'étendre à d'autre types d'intermédiaires informationnels, une telle extension nécessite que ces intermédiaires incarnent un danger similaire pour la vie privée des individus. Par exemple, cela sera le cas lorsqu'ils permettent à leur utilisateurs, lors d'une recherche portant sur un non, d'obtenir un "aperçu structuré" leur permettant d'établir un profil plus ou moins détaillé de la personne concernée. (CJUE, 2014, at pars. 37, 80; Article 29 DPWP, 2014, at par. 17-18).

II. B. La blockchain

Une blockchain est une base de données décentralisée qui possède quelques caractéristiques spécifiques. En premier lieu, une blockchain fonctionne comme un réseau décentralisé en pair-à-pair, qui n'est ni possédé ni contrôlé par une autorité centrale/centralisée. Chaque pair du réseau possède une copie de la blockchain, et il contribue avec ses capacités de calculs à la sécurité et au maintien des opérations du réseau. En second lieu, une blockchain est une base de données à laquelle on ne peut que faire des ajouts : la seule possibilité est d'ajouter de l'information, dans l'ordre chronologique ; il est impossible de modifier ou supprimer une information une fois qu'elle est enregistrée. Enfin, une blockchain est un registre certifié, qui repose sur la cryptographie pour assurer que toutes les données enregistrées sont cohérentes, et ont été validées par la majorité des noeuds du réseau (Nakamoto, 2008).

Les avantages de cette technologie sont évidents, notamment sur la question de l'intégrité des données et de leur certification. Puisque personne ne peut modifier l'information stockée dans une blockchain a posteriori, la blockchain peut prouver qu'un document spécifique a existé, ou qu'un événement est arrivé à un moment T (Lemieux, 2016).

En revanche, la blockchain soulève de nombreuses inquiétudes, en majorité liées à l'inaltérabilité de l'information contenue (Vogel, 2015). La technologie fonctionne de telle manière qu'il serait impossible de supprimer du contenu illicite ou inadéquat s'il venait à être

stocké dans une blockchain sans une action coordonnée de la majorité des noeuds individuels. Et dans la mesure où elles peuvent contenir des informations inadéquates, non pertinentes ou excessives, les blockchains pourraient également devenir un défi posé au droit à l'oubli. Puisqu'aucun acteur central n'est là pour contrôler le réseau, personne ne peut être tenu responsable de l'application du droit à l'oubli dans la blockchain (Umeh, 2016)

III. Les interactions entre la blockchain et le droit à l'oubli

III. A. L'application du droit à l'oubli à la blockchain Bitcoin

En partant des éléments expliqués ci-dessus, il pourrait être intéressant de se questionner sur l'éventuelle application du droit à l'oubli à la blockchain Bitcoin. Si, par hypothèse, un individu avait opéré une transaction gênante dans le passé, comme une inscription à un site du type Ashley Madison, pourrait-il légitimement demander la suppression de cette transaction du registre Bitcoin ?

Puisque le droit à l'oubli ne s'applique présentement qu'aux moteurs de recherche généralistes, le premier réflexe est de répondre par un "non" catégorique. On peut néanmoins se demander dans quelle mesure le droit à l'oubli pourrait être étendu à la blockchain Bitcoin par analogie, la possibilité d'une telle extension n'étant, on le rappelle, non exclue d'emblée si l'intermédiaire informationnel porte un danger suffisant pour la vie privée des individus, et notamment par la diffusion d'un profil public lorsqu'on entre le nom d'une personne. Ce dernier élément de l'argument sous-tend cependant que l'exercice du droit à l'oubli exige un élément de publicité et d'accessibilité au public: c'est d'ailleurs pourquoi les moteurs de recherche ont l'obligation de prévenir à l'affichage de certains résultats mais ne sont pas pour autant amenés à retirer les liens correspondants de leur index ni à empêcher leur diffusion lors de l'emploi d'autres mots-clés que des noms (Reymond, 2016, at 41-43). Par conséquent, une personne ne devrait pas pouvoir l'invoquer pour demander la suppression d'un lien non public contenu dans une base de données en ligne; le droit à l'oubli ne peut donc pas être invoqué pour faire supprimer certaines informations disponibles sur internet : il ne sert qu'à protéger les citoyens de la perspective d'être indéfiniment liés à des contenus faciles à trouver sur Internet, comme dans le cas où un employeur taperait le nom de ses recrues potentielles au moment de l'embauche (Rustad & Kulevska, 2016, at 365-366).

Sur deux aspects, la blockchain Bitcoin ne répond pas à ces exigences. Premièrement, dans la mesure où le réseau Bitcoin met en relation des pseudonymes, l'information liée à la transaction notée dans le registre décentralisé ne permet pas l'identification des utilisateurs du réseau, et ne donne aucune information sur le contexte général de l'échange (De Filippi, 2016). Les individus qui font des échanges en Bitcoin ne sont désignés dans la blockchain qu'à travers leur adresse Bitcoin, un identifiant global sous forme d'une chaîne de caractères de ce type : "37WctrDb1G1orXhJ8vgx7zS2WCuSuBk6EQ". Aucune autre information n'est disponible, ni sur leur identité hors ligne, ni sur la nature de leur transaction. Ainsi, les informations stockées dans la blockchain Bitcoin ne pose pas d'effet visible sur la vie privée des personnes qu'elle

répertorie, ou en tout cas dans aucune mesure comparable à un moteur de recherche. Deuxièmement, les informations stockées sur la blockchain ne sont pas accessibles librement, ou tout du moins avec bien moins d'aisance qu'avec un site web ou un moteur de recherche. De par sa nature en tant que base de données décentralisée distribuée sur un réseau d'ordinateurs, la blockchain Bitcoin n'est véritablement accessible qu'aux seuls utilisateurs ayant les moyens logistiques et informationnels leur permettant d'installer les logiciels nécessaires pour obtenir l'accès au réseau et à en miner les données y contenues. Évidemment, cette tâche requiert une connaissance et des efforts incomparables à ceux fournis pour consulter un site internet.

Bien entendu, nous n'entendons pas par là que le droit à l'oubli ne peut pas s'appliquer aux intermédiaires qui fournissent une interface permettant de consulter directement la blockchain Bitcoin. Le site internet blockchain.info, par exemple, fournit un accès simple et mis à jour en temps réel sur l'état du registre Bitcoin, quoiqu'il ne lie aucune donnée de transaction à des informations qui permettraient d'identifier des personnes.

A l'inverse, si le site internet permettait de lier des adresses Bitcoin à des noms et prénoms réels, et de permettre la recherche d'entrées par noms dans ce cadre, nous aurions potentiellement un cas d'application du droit à l'oubli. Cependant, même dans ce cas, l'obligation de déréférencement ne s'appliquerait qu'à ce site en particulier, et uniquement en vertu de sa fonction de portail direct de recherche dans la blockchain Bitcoin. Le droit à l'oubli ne concernerait donc en aucun cas la blockchain Bitcoin en tant que telle.

III. B. Le droit à l'oubli appliqué à d'autres usages de la blockchain (le cas Steem.it)

La blockchain Bitcoin n'est qu'un exemple parmi tant d'autres des usages possibles de cette technologie émergente. A la suite de la popularisation du Bitcoin, de nombreuses autres applications basées sur la blockchain ont été développées, chacune avec leurs caractéristiques propres (Crosby & al., 2016). Pour le moment, la plupart d'entre elles relèvent du domaine de finance, mais quelques unes apparaissent dans le domaine de la création et de la distribution de contenu (Swan, 2015). Steem.it est un exemple emblématique de cette tendance; il s'agit une plateforme de publication et de réseau social basée sur la blockchain dont le principe tient à la favorisation et à la rémunération, à l'aide d'une monnaie virtuelle, des contributions de ses utilisateurs. Ces contributions peuvent prendre plusieurs formes, allant de la publication de contenu original (des billets de blog, des vidéos, des images, etc.) à la conservation active de la plate-forme par l'appréciation du contenu soumis par d'autres utilisateurs (commentaire, votes positifs et négatifs...)

Steem.it est basé sur sa propre blockchain, dans laquelle chaque contribution est stockée grâce aux métadonnées appropriées (identité du contributeur, commentaires, votes reçus). Le contenu textuel est directement stocké dans la blockchain, et les images et vidéos sont hébergées par des solutions tierces : seul le lien vers ce contenu est stocké dans la blockchain. On pourrait affirmer que la blockchain Steem.it pourrait être concernée par le droit à l'oubli, au

moins dans la mesure où certains pourraient l'utiliser pour extraire des informations liées à des individus spécifiques.

Cependant, comme décrit ci-dessus, le contenu enregistré dans une blockchain ne peut plus être ni modifié, ni supprimé par qui que ce soit dans la mesure où la technologie de la blockchain est, par essence, inaltérable. Ainsi, l'intégralité du contenu enregistré dans la blockchain Steem.it est impossible à censurer. Et puisqu'il n'y a aucune autorité centrale qui gère le réseau, aucun gouvernement ne peut adresser de requête visant la suppression d'informations sensibles ou de contenu considéré comme illicite.

Cela étant, la plupart des utilisateurs de Steem.it n'interagissent pas directement avec sa blockchain, mais se contentent d'accéder aux contenus via son site internet, qui est, lui, géré de manière centralisée. En effet, le site internet de Steem.it collecte des informations sur les contribution de la blockchain Steem.it, et les présente de manière claire et accessible, avec le nom des contributeurs. ~~Bien entendu,~~ Tous les contenus ne sont pas affichés sur le site : à la suite de l'évaluation de ces contenus, ceux qui ont reçu des votes négatifs finissent par disparaître du site - quoiqu'ils restent stockés dans la blockchain. En ce sens, le site internet de Steem.it peut être considéré comme un intermédiaire (ou plutôt un infomédiaire) qui collecte les informations d'une base de données et les rend accessibles au public en fonction de critères spécifiques. En tant que tel, on pourrait tout à fait invoquer le droit à l'oubli pour demander aux administrateurs du site internet de Steem.it de retirer un contenu qui divulguerait des informations inadéquates ou excessives sur une personne.

L'application du droit à l'oubli pourrait cependant être difficile dans la mesure où le site de Steem.it, tout centralisé qu'il soit, manque d'une structure centralisée de modération et d'administration. La modération est effectuée par les utilisateurs eux-mêmes, qui prennent la responsabilité de donner des votes négatifs aux contenus qu'ils considèrent comme inappropriés. Autoriser la suppression d'un contenu qui n'aurait pas reçu de votes négatifs de la part de la communauté de Steem.it contreviendrait à leur politique et pourrait dissuader leurs utilisateurs de continuer à utiliser le site internet. De plus, dans la mesure où toutes les informations de la blockchain de Steem.it sont publiques, il est impossible d'empêcher des tiers de développer leurs propres versions alternatives (de type darknet) du site de Steem.it et de proposer un accès exhaustif à la blockchain, y compris aux informations indésirables, à ceux qui voudraient réellement y avoir accès.

IV. L’exécution du droit à l’oubli sur la blockchain

A. Problématique

Imaginons une plateforme fictive basée sur la blockchain qui fonctionnerait comme un LinkedIn décentralisé, nourri par les contributions de ses utilisateurs. Cette blockchain serait un registre dans lequel n'importe qui pourrait ajouter des informations au sujet d'une personne en particulier - par exemple, en fournissant des liens vers un contenu déjà disponible sur Internet. Toute personne qui souhaiterait en savoir plus sur un individu pourrait parcourir le contenu

accumulé par l'entier des utilisateurs. Dans un tel scénario, il va sans dire que le droit à l'oubli pourrait légitimement être invoqué, car ce service permettrait à n'importe qui d'accéder à une sorte de profil public de la personne, qui pourrait inclure des liens ou des références à des informations "inexactes, inadéquates ou excessives". Certes, on pourrait argumenter que l'élément de publicité n'est pas rempli, car ces informations seraient moins immédiatement consultables que si elle étaient indexées par un moteur de recherche ou même disponibles sur le véritable LinkedIn, mais dans l'hypothèse où la blockchain serait accessible à n'importe qui, il reste vraisemblable que le droit à l'oubli puisse être invoqué pour demander la suppression de certains liens y contenus.

L'application hypothétique du droit à l'oubli à une telle plateforme soulève de nombreuses interrogations quant au degré de responsabilité des acteurs qui la font vivre, ainsi qu'à leurs devoirs. Contrairement au plateformes traditionnelles qui fonctionnent sur un modèle centralisé et dont on peut facilement identifier le fournisseur d'accès, un réseau blockchain est opéré par chacun des noeuds du réseau, de manière décentralisée - il n'existe aucune entité centrale ayant l'autorité ou la capacité technique d'ajouter, supprimer ou modifier les informations stockées dans la blockchain.

Ainsi, on peut légitimement se demander comment un LinkedIn décentralisé pourrait appliquer le droit à l'oubli dans le cas où un citoyen européen demanderait la suppression d'un lien contenu dans la blockchain. En l'absence d'intermédiaire, qui serait responsable d'assurer la mise en oeuvre de cette requête ? Et qui serait tenu, le cas échéant, responsable d'un tel manquement au droit l'oubli ?

A première vue, dans la mesure où la blockchain est par essence inaltérable et que le stockage d'informations est irréversible, demander la suppression d'un élément de la blochchain semble tout simplement absurde, puisqu'impossible à réaliser techniquement. Et puisque personne n'a le pouvoir de supprimer unilatéralement les données d'une blockchain, personne ne peut être tenu responsable de la non-suppression de certaines informations.

Cependant, résumer ainsi les liens entre blockchain et droit à l'oubli est assez réducteur. De fait, l'action coordonnée des noeuds actifs du réseau permet de supprimer certaines données d'une blockchain . Dans le cas du Bitcoin, par exemple, deux transactions apparemment valides mais incompatibles l'une avec l'autre (l'exemple classique est une double dépense des mêmes fonds de départ) seront sujettes au protocole de consensus décentralisé de Bitcoin, qui permettra de décider de la transaction à conserver et de celle qu'il faut supprimer (Nakamoto, 2008) - alors que cela implique clairement de changer l'état actuel de la blockchain. On pourrait imaginer que cette technique s'applique au retrait de contenu illégal (contenus sous copyright, discours d'incitation à la haine ou pédopornographie) d'une blockchain publique. S'il y a consensus sur le fait que certains contenus soient inappropriés vis-à-vis de la plateforme, il est techniquement possible de les retirer de la blockchain. Bien tendu, c'est trouver ce consensus au sein d'un réseau décentralisé qui pose la principale difficulté (De Filippi & Loveluck, 2016), et ne pas y parvenir a parfois des conséquences inattendues.

IV. B. Ethereum et ses implications sur le droit à l'oubli

L'exemple récent du hack de TheDAO nous fournit une bonne illustration de ces différentes problématiques : à la suite de ce hack, la blockchain Ethereum s'est séparée en deux réseaux différents : Ethereum et Ethereum Classic. Cet événement n'impliquait certes aucune question de vie privée ou de liberté d'expression, mais son analyse permet d'avoir un aperçu pertinent des enjeux du caractère inaltérable de la blockchain.

Ethereum est un plateforme blockchain de cryptomonnaie semblable au Bitcoin. Lancée en juin 2015, elle permet à ses utilisateurs d'échanger des jetons Ether (ou ETH). Contrairement au Bitcoin, la blockchain Ethereum inclut un langage Turing-complet, qu'on peut utiliser pour inclure du logiciel dans ses transactions. Pour donner un exemple concret : Alice pourrait vouloir mettre en place un versement régulier à Bob à chaque fois qu'un événement spécifique survient. En intégrant ces instructions à la blockchain, le paiement sera effectué comme prévu, sans qu'Alice ni Bob n'aient besoin de faire quoique ce soit de leur côté. Ces possibilités, qui existent sous la dénomination de contrats intelligents (smart contracts), peuvent concerner des conditions très simples ou des montages logiciels très complexes.

Dans ce contexte, TheDAO (abréviation de Organisation Autonome Décentralisée) a été lancé en avril 2016. L'objectif de TheDAO était de mettre en place une organisation complètement automatisée, dont les règles de fonctionnement s'appliquaient dans le cadre des contrats intelligents. Le code permettait à des investisseurs d'envoyer des fonds dans un portefeuille commun, et de recevoir un nombre de jetons proportionnel à leur investissement, ce qui leur permettait de participer à la gouvernance et à la prise de décisions de l'organisation en question. Un mois après son lancement, l'organisation avait déjà attiré 150 millions d'Ether d'investissement. Un tiers de la valeur de l'argent investi fut dérobé le 18 juin 2016 par un attaquant non-identifié qui avait exploité une vulnérabilité dans le code des contrats intelligents.

Devant l'indignation provoquée par cet événement, la communauté Ethereum a décidé d'intervenir en mettant en place un action coordonnée pour effectuer des modifications dans la blockchain Ethereum (un "hard fork"). Tous les participants actifs du réseau ont été invités à passer à une version alternative du registre, dans lequel les fonds qui avaient été volés n'appartenait plus à l'attaquant mais étaient déposés dans un compte créé pour l'occasion pour que les investisseurs récupèrent leur argent. Cette solution n'a pas fait l'unanimité : quelques utilisateurs ont avancé que cet action compromettait l'inaltérabilité de la blockchain et ont refusé d'adopter cette version alternative. Cet événement a conduit à l'émergence d'une blockchain Ethereum alternative - Ethereum Classic - qui rejettait le hard fork et conservait la blockchain originale.

Il y a de nombreux enseignements à tirer de cette histoire. Avant tout, il donne la preuve que les blockchains peuvent être modifiées. Si elle se retrouve face à des sanctions économiques ou juridiques, la communauté qui fait vivre une blockchain peut prendre la décision d'intervenir collectivement pour censurer une transaction spécifique ou supprimer des informations y contenues. Mais la nécessité de respecter les lois européennes de protection des données

seront-elles une incitation suffisante ? La question reste ouverte. Le second enseignement à tirer de l'exemple d'Ethereum est le constat que même si la majorité de la communauté souhaite collaborer avec les autorités chargées de faire respecter la loi, il est difficile de faire disparaître les informations de la blockchain sans le consensus de toute la communauté. Il suffit d'un simple désaccord pour que la blockchain se sépare en deux réseaux différents.

V. Conclusion

L'apparition de la blockchain va avoir d'indéniables conséquences sur la régulation de la mise à disposition des informations, notamment d'un point de vue technique : les données d'une blockchain ne peuvent être modifiées ni supprimées. Il est cependant plus difficile d'évaluer l'impact de l'émergence de ces nouvelles technologies sur la possibilité de faire appel au droit à l'oubli. De fait, ce n'est pas la résistance à la censure de la blockchain qui pose directement problème : le droit à l'oubli ne peut pas, du moins dans sa version actuelle, donner lieu à une demande de suppression de contenu, mais uniquement le déréférencement de ce contenu. Bien entendu, il n'est pas exclu que des citoyens européens puissent légitimement invoquer le droit à l'oubli dans le cas où des liens de ce type seraient stockés dans une blockchain et où ils permettraient à un large groupe d'utilisateurs d'accéder à des informations inexactes, inadéquates ou excessives. Dans ce cas précis, les spécificités techniques de la blockchain risqueraient de poser problème à l'application du droit à l'oubli. Dans la mesure où la blockchain n'est pas gérée par un administrateur central, aucune entité n'a l'autorité ni la capacité de modifier ou supprimer unilatéralement des éléments de la blockchain. La seule possibilité de modifier ou supprimer les données incriminées implique un accord et une action coordonnée de l'intégralité - ou au moins d'une large majorité - des noeuds actifs d'une blockchain, qui effectuerait de manière cohérente les modifications nécessaires (Wright & De Filippi, 2015). Bien entendu, l'exemple d'Ethereum nous a montré que même s'il existait un large consensus autour d'une modification de la blockchain, il suffit d'une petite minorité qui rejette la modification pour qu'elle puisse maintenir une version non-modifiée de la blockchain.