HAL
open science

Le droit à l'oubli : Présentation du projet DAO

Annie Blandin-Obernesser, Maryline Boizard, Sébastien Gambs, Guillaume Piolle

To cite this version:

Annie Blandin-Obernesser, Maryline Boizard, Sébastien Gambs, Guillaume Piolle. Le droit à l'oubli : Présentation du projet DAO. 4ème Atelier sur la Protection de la Vie Privée (APVP'13), Jun 2013, Les Loges en Josas, France. hal-00845780

HAL Id: hal-00845780

https://inria.hal.science/hal-00845780v1

Submitted on 17 Jul 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

LE DROIT A L'OUBLI : présentation du projet DAO

Auteurs : Annie Blandin (Télécom Bretagne), Maryline Boizard (Univ. de Rennes 1), Sébastien Gambs (Univ. de Rennes 1 – INRIA) et Guillaume Piolle (Supélec)

La notion d'oubli correspond à deux réalités bien distinctes. D'une part, **le fait d'oublier** lors d'une défaillance de la mémoire, qui renvoie à un acte involontaire pouvant être préjudiciable à son auteur ou à un tiers et qui, sauf circonstances exceptionnelles, est sanctionné lorsqu'il constitue la violation d'une obligation légale ou conventionnelle. D'autre part, **le droit à l'oubli** qui consiste en une prérogative qu'aurait chaque individu d'exiger que ne soient plus accessibles à tous certains événements ou données le concernant. Il s'agit donc d'une soustraction à la mémoire collective (et éventuellement au patrimoine informationnel de l'entreprise). Cette soustraction n'est cependant pas totale, car même si telle est la volonté de l'individu, il reste débiteur d'obligations envers la société à laquelle il appartient. Par conséquent, si un droit à l'oubli doit être consacré, il ne saurait l'être de façon absolue.

A l'heure du tout numérique, le droit à l'oubli évoque nécessairement l'effacement de données informatiques et renvoie au droit de l'Internet et des réseaux. Si l'idée d'un droit à l'oubli numérique n'est pas nouvelle, elle se concrétise pour la première fois de façon spécifique dans la proposition de règlement du Parlement européen et du Conseil relatif à la protection des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) du 25 janvier 2012 qui consacre un article au droit à l'oubli et à l'effacement (article 17), lui-même inséré dans une section 3 concernant la rectification et l'effacement. Cette section fait partie du chapitre relatif au droit des personnes.

L'ampleur du phénomène, son actualité et ses différentes manifestations nous conduisent à nous interroger sur la manière dont les dispositifs actuels devraient évoluer pour répondre aux défis du numérique. Dans ce contexte, la réflexion peut être menée sous trois angles, un angle juridique (1), un angle sociologique (2) ainsi qu'un angle technique (3). Dans ce document, nous présentons principalement les pistes de réflexion qui sont menées dans le cadre du projet DAO (Droit À l'Oubli) sous l'angle juridique et informatique. Ce projet est conduit sous l'égide du ministère de la justice.

1. L'approche juridique du droit à l'oubli

Le droit à l'oubli est consacré de manière éparse dans différents domaines du droit, mais peut-on imaginer un droit à l'oubli numérique autonome, et si oui quels en seraient les contours, et comment garantir son effectivité ?

1.1 Les manifestations du droit à l'oubli dans le droit positif

Il convient de distinguer les règles concernant l'oubli d'informations, éventuellement sous forme numérique, et celles concernant les informations personnelles dont le lien avec le numérique est très étroit. L'étude des **règles consacrant directement ou indirectement un droit à l'oubli** en dehors du contexte numérique permet de mieux comprendre les enjeux du droit à l'oubli et de pointer les limites d'une organisation disparate de ce droit.

De façon indirecte, le droit à l'oubli est sous-jacent dans les mécanismes de prescription extinctive et dans certains principes protecteurs de la personnalité. Ainsi la prescription éteint-elle le droit de celui qui pouvait exercer un droit en justice et qui ne l'a pas fait dans le temps prévu par la loi. La règle est justifiée en droit civil par des motifs de paix sociale, d'ordre public et de sécurité juridique. En droit pénal en revanche, elle est dictée par le droit à l'oubli[1].

De même, les droits fondamentaux de la personne, tels que le droit au respect de la vie privée garanti par les articles 9 du Code civil et 8 de la CEDH, permettent à la jurisprudence de condamner des pratiques allant à l'encontre du droit à l'oubli[2]. Il s'agit néanmoins de fondements qui n'ont pas été imaginés pour garantir un droit à l'oubli, ce qui laisse planer des incertitudes sur les contours de la notion.

---

[1] C. Costaz, Le droit à l'oubli, Gaz. Pal 1995, p. 961. R. Merle et A. Vitu, Traité de droit criminel, Procédure pénale, 4è ed., Cujas, n° 818.

[2] Notamment, CA Paris 15 sept. 2000 : Gaz. Pal. 2001, n° 270 p.18. Cass. Civ. 1ère, 7 mai 2008, D. 2008, AJ 1481, J. Hauser

De façon directe, la loi du 29 juillet 1881 sur la liberté de la presse, complétée par l'ordonnance du 6 mai 1944, fait jouer de l'effet du temps en privant de la possibilité d'établir la véracité de faits diffamatoires lorsque leur imputation remonte à plus de dix ans.

S'agissant spécifiquement (mais pas exclusivement) du contexte numérique, la loi « informatique et libertés » du 6 juillet 1978 esquisse les contours d'un droit à l'oubli se traduisant par une durée de conservation des données personnelles n'excédant pas « la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées » et par un droit de retrait ou un droit d'opposition à l'utilisation de ces données. Surtout, la loi prévoit un droit à l'effacement, comme composante du droit d'accès, mais dont la portée est limitée car on ne peut l'invoquer que dans le cas où les traitements de données ne sont pas conformes.

En ouvrant la possibilité aux personnes de demander l'effacement dans des hypothèses très larges, la proposition de règlement européen pose de nombreuses questions : la protection des données doit-elle permettre de lutter contre toute atteinte liée à l'usage des données personnelles ? Jusqu'où convient-il d'aller ? Doit-on traiter par exemple de la même façon des données a priori banales, retraçant des événements du quotidien d'une personne diffusées par elle-même sur Facebook, Youtube ou Twitter, des données médicales et des informations à caractère pénal ?

Bien qu'inscrit dans l'ordre juridique, le droit à l'oubli est donc plutôt conçu pour faire face à des situations particulières du monde numérique. Or, il est légitime de se questionner sur la capacité d'une telle approche permette de répondre à des situations inédites qui ne manqueront pas d'arriver avec le développement de nouvelles technologies non anticipées.

1.2. La détermination des contours d'un droit à l'oubli

Cette photographie des dispositifs existants doit nous permettre de **délimiter les contours du droit à l'oubli**. Dans cette phase de réflexion, il conviendra de répondre à quatre questions :

Que peut-on protéger par le droit à l'oubli numérique ? Il s'agit d'identifier la nature des informations dont un individu peut demander le retrait ou à la diffusion desquelles il peut s'opposer. Actuellement, les informations visées sont les données à caractère personnel, ce qui pose à la fois la question de la définition de ces données et de la diversité des données concernées. En effet, celles-ci sont de tous ordres et de nature très diverses, ce qui implique de faire des incursions dans le doit médical, dans le droit pénal, dans le droit de la preuve ou encore dans le droit du travail. Se pose par ailleurs le problème de la distinction entre sphère privée et publique. On s'accorde en effet à considérer que la vie publique concerne la vie politique, professionnelle, les affaires judiciaires, les manifestations ou encore certains faits divers exceptionnels[3]. Mais peut-on envisager que, par l'effet de l'écoulement du temps, le droit à l'oubli puisse être invoqué pour des événements de la vie publique de la personne ? De même, comment traiter une information, constitutive de propos diffamatoires, diffusée de façon privée sur Facebook et ultérieurement divulguée publiquement par un tiers à la suite d'un simple « copier-coller » ? Faute de disposition adéquate, on assiste à un élargissement jurisprudentiel de la notion de vie privée[4]. La frontière entre vie privée et vie publique est parfois ténue et le droit à l'oubli agite le spectre de la censure.

Qui peut-on protéger par le droit à l'oubli ? La personne, certes, mais doit-on offrir au majeur sain d'esprit la même prérogative qu'au mineur ou au majeur protégé ? Un personnage public peut-il prétendre à un droit à l'oubli aussi étendu qu'une personne moins exposée ? L'appréhension du droit des personnes, et notamment du droit des incapacités, est ici déterminante.

Contre quoi le droit à l'oubli peut-il protéger ? Le droit à l'oubli concerne assurément la collecte et la diffusion d'informations à caractère personnel mais *quid* de la conservation et de l'exploitation de ces données? En amont, au stade de la collecte et de la diffusion, des mesures comme l'anonymisation des

[3] Voir en ce sens, G. Haas et O. de Tissot, Le paradoxe du droit à l'oubli. Expertises mars 2005, p.105.

[4] L. Marino, Les nouveaux territoires des droits de la personnalité, Gazette du Palais 2007, n 139, p. 22. A. Lepage, La notion de vie privée au sens de l'article 8 de la CEDH ne cesse de prendre de l'ampleur (au sujet de l'aff. Rotaru c/ Roumanie du 4 mai 2000), D. 2001, p. 1988.

décisions de justice permettent d'éviter une diffusion compromettante. En aval, le législateur a joué sur la durée de conservation des données personnelles en la réduisant mais c'est encore jugé insuffisant par certains.

Contre qui le droit à l'oubli peut-il protéger ? Le droit à l'oubli, tel qu'il est conçu aujourd'hui, n'est pas opposable à tous. Il se heurte, d'une part, à l'intérêt général, lequel sert de justification aux atteintes les plus flagrantes au droit des personnes et au droit à l'oubli en particulier. C'est bien la priorité donnée par l'État à la sécurité qui a légitimé la mise en place du système de traitement des infractions et le fichier des empreintes génétiques. Le droit à l'oubli se heurte également au devoir de mémoire et à la liberté d'expression, souvent invoqués par les journalistes ou par les auteurs de fictions du réel[5]. La jurisprudence se montre assez favorable à la préservation de ces grands principes qui l'emportent bien souvent face au droit au respect de la vie privée. Les journalistes ou auteurs disposent donc d'une certaine liberté d'action, mais qu'en est-il par exemple des droits de l'employeur face aux données personnelles concernant le salarié ?

Les réponses à ces questions devraient nous permettre de prendre position quant à la délimitation d'un droit à l'oubli. Mais pour que la consécration du droit à l'oubli ait du sens, il faut en garantir l'effectivité.

1.3 – L'effectivité du droit à l'oubli

Une nouvelle réforme du droit de la protection des données personnelles est engagée à l'échelon européen. La Commission européenne lançait en novembre 2010 une consultation publique sur les questions relatives à la protection des données personnelles dans le but de redéfinir le cadre de la protection des données et de réviser la directive de 1995. Il en ressort que les Européens acceptent le fait que le traitement des données personnelles se développe, mais souhaitent bénéficier d'outils et de règles permettant d'effacer, à n'importe quel moment, les informations mises en ligne. Ils veulent aussi que leur accord soit d'abord pris en compte avant toute collecte ou traitement. La France n'est pas en reste avec la proposition de loi *visant à mieux garantir le droit à la vie privée à l'heure du numérique*[6].

L'effectivité du droit à l'oubli sera étroitement liée à sa place dans l'échelle des normes et aux modalités dont il sera assorti.

D'une part, la **place du droit à l'oubli dans l'échelle des normes** est fondamentale dans la mesure où la diffusion des informations sur la toile, par définition, ne connaît pas de frontières géographiques. Le droit à l'oubli circonscrit au territoire national aurait incontestablement une effectivité limitée. Néanmoins, la perception des atteintes au droit des personnes peut différer d'un pays à l'autre. Aux États-Unis par exemple, les lois antiterroristes imposent aux compagnies aériennes de divulguer les informations les plus diverses sur leurs passagers, permettant la réalisation de fichiers aux données précises, ce qui heurte certaines législations européennes. Cette disparité favorise l'impunité. Il est ainsi très aisé d'implanter son siège social dans un pays peu regardant, pour se mettre à l'abri d'actions judiciaires tendant à obtenir la suppression d'une donnée privée.

S'interroger sur la place du droit à l'oubli dans l'échelle des normes, c'est également le positionner parmi les dispositifs juridiques existants, ce qui implique de déterminer si le droit à l'oubli peut être un élément parmi d'autres des droits garantissant le respect de la vie privée ou si, au contraire, il convient de le sortir de la sphère de ce droit pour l'ériger en droit autonome.

D'autre part, les **modalités de mise en œuvre** du droit à l'oubli doivent être déterminées avec soin car elles sont le garant de la réalité du droit.

Ainsi, l'effectivité du droit à l'oubli ne sera assurée que par une *information pertinente de son bénéficiaire*. Cette information est destinée, de façon préventive, à permettre à chacun de mesurer les conséquences de la diffusion, par elle-même, de certaines informations au public et, de façon curative, à faire connaître aux victimes la nature et l'étendue de leur droit face à une atteinte dont elles pourraient

[5] A. Fourlon, « Toute ressemblance avec des personnages existant ou ayant existé… » est-elle constitutive d'une atteinte aux droits de la personnalité ? Comm. Comm. Electr. 2007, étude 5.

[6] Proposition de loi adoptée par le sénat le 6 nov. 2009 (sénat n° 93), transmise à l'AN en 1ère lecture le 24 mars 2011 (A.N. n°2387).

être l'objet. Une démarche en ce sens est engagée dans le projet de loi tendant à moderniser la loi de 1978. L'article 1er prévoit d'ajouter au Code de l'éducation un alinéa qui intègre au programme d'éducation civique un enseignement « sur les risques liés aux usages des services de communication au public en ligne ».

L'effectivité du droit à l'oubli peut également être améliorée par *l'implication des acteurs du marché* à travers la réalisation de chartes ou de codes de bonne conduite par lesquels ils prendraient un certain nombre d'engagements permettant d'agir préventivement[7]. C'est une des voies choisie par la France puisqu'elle s'est dotée d'une *Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche.* Les codes de bonne conduite ont néanmoins leurs limites et ne privent pas d'une réflexion sur l'adoption de sanctions adéquates. Il faut engager une réflexion sur la nature et l'étendue des sanctions envisageables, de sorte qu'elles soient dissuasives. A titre d'exemple, l'association Lexeek qui a publié sur son site des décisions judiciaires de plusieurs tribunaux sans les anonymiser, vient de recevoir une injonction de la CNIL de cesser le traitement d'informations personnelles assortie d'une amende de 10 000 euros.

2. L'approche sociologique du droit à l'oubli

C'est en deuxième lieu une approche sociologique en articulation avec l'équipe de juristes qui permettra de définir les pratiques et les perceptions du droit à l'oubli par les intéressés. Cette perception paraît essentielle dans la détermination de la nécessité d'un droit à l'oubli et, subséquemment, dans l'identification des outils à mettre en œuvre. Il s'agit ici d'identifier le ressenti du public face à la conservation et à l'exploitation de données personnelles et de mesurer la conscience qu'il peut avoir de l'impact d'une telle conservation en confrontation avec l'observation de ses pratiques.

Cette étude sociologique examinera d'une part les discours et, d'autre part, les pratiques réelles des internautes interrogés, afin de mesurer l'écart entre les deux et de recueillir les justifications de cet écart, formulées par les acteurs eux-mêmes. L'étude pourra partir de l'enquête TNS Sofres parue le 8 novembre 2011 sur « Les pratiques numériques des Français » ou encore l'enquête de la Caisse des dépôts et consignation sur la confiance dans le numérique. Ces enquêtes quantitatives montrent des clivages par tranches de 3 à 5 ans et non plus par PCS. Elles montrent également que les plus jeunes (14 – 17 ans) ont intégré dans les discours le risque, la question de la crédibilité de la source ou la menace pour la vie privée mais que ce sont eux qui ont les pratiques les plus assidues et les plus diversifiées. Ces enquêtes pointent des dimensions nouvelles qui demandent à être complétées par une enquête qualitative sur le terrain telle que nous le proposons. Il semblerait que les plus jeunes aient un rapport lucide et moins candide sur les risques liés à Internet et à l'exploitation des données personnelles par des acteurs majeurs des réseaux sociaux. Comment ajustent-ils leurs pratiques en conséquence? C'est ce que devrait nous dévoiler le résultat de l'étude sociologique menée sur le terrain.

3. L'approche technique du droit à l'oubli

Enfin, il paraît illusoire de considérer l'effectivité d'un potentiel droit à l'oubli sans en évaluer les possibilités de mise en œuvre technique. Il convient donc d'évaluer la capacité réelle de l'informatique à faire disparaître une information.

Pour un être humain, la mémorisation d'une information demande souvent un effort conscient, alors que l'oubli est au contraire une phénomène naturel qui intervient inconsciemment. Par contraste, au niveau des ordinateurs, qui sont conçus pour stocker (et traiter) de l'information, c'est le fait d'oublier qui constitue un défi technique.

À l'échelle d'une machine unique, il est déjà très difficile de faire disparaître une information de manière efficace si elle a été stockée sur un disque dur standard, sans précautions particulières. Ainsi en pratique, la suppression d'un fichier consiste généralement en l'effacement d'une entrée dans un table d'indexage. Il ne s'agit donc pas d'un écrasement réel de la donnée elle-même. Pour réaliser cet effacement, il existe des logiciels dédiés, qui sont par exemple référencés dans les listes de produits

[7] Charte du 13 oct. 2010 sous l'égide de N. Kosciusko-Morizet, alors Secrétaire d'Etat à l'économie numérique.

certifiés (selon les « Critères Communs »[8] ou la « Certification de Sécurité de Premier Niveau »[9]) par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Ces logiciels, parfois appelés « anti-forensiques », sont souvent utilisés lorsqu'un risque spécifique relatif à la rémanence des données est identifié, comme par exemple lors du remplacement d'un disque dur contenant des données sensibles.

Actuellement, le risque le plus prégnant et le plus difficile à résoudre techniquement est celui lié à l'interconnexion des systèmes d'information et des réseaux d'ordinateurs. Un verrou majeur concerne le traçage et le contrôle du devenir d'une donnée une fois qu'elle a été transmise à un tiers. Plus particulièrement, lors de la mise en œuvre technique du droit à l'oubli, il semble important de pouvoir garantir qu'une entité distante a réellement supprimé une donnée qui lui a été confié, sans préalablement en avoir faite de copies et sans l'avoir transmise à un tiers. Malheureusement, à l'heure actuelle, il n'existe aucun mécanisme technique qui peut dans l'absolu offrir une telle garantie sur la copie ou la conservation possible d'une donnée.

Considérons par exemple un interlocuteur distant qui a accès à une information sous la forme d'un texte ou d'une image affichée sur son écran. Même si au niveau de son ordinateur un mécanisme est mis en place pour lui interdire de faire une copie de cette donnée, il lui est toujours possible de prendre une photographie de son moniteur via un appareil indépendant de son ordinateur. Ensuite, cet interlocuteur pourra disposer comme bon lui semble de la copie obtenue. Cette simple observation exclut de pouvoir proposer une mise en œuvre du droit à l'oubli sur des données numériques qui serait à la fois totalement générique et parfaitement effective. Cependant, ce résultat d'impossibilité, qui s'appuie sur un scénario relativement spécifique, ne doit pas condamner tout démarche dans ce sens. En particulier, il reste possible de concevoir des implémentations techniques du droit à l'oubli, se fondant sur des solutions logicielles, matérielles ou même sur une combinaison des deux, pouvant sous certaines conditions fournir à un individu un certain niveau de garantie sur la suppression de données dont il est à l'origine ou le concernant. Les approches que nous évoquons ci-après sont des exemples de telles implémentations.

3.1. Les limites de l'anonymisation

Pour les responsables de traitements, la notion de droit à l'oubli fait écho à l'obligation de supprimer les données à caractère personnel qui ne sont plus absolument nécessaires à la finalité pour laquelle elles ont été collectées. Théoriquement, on peut anonymiser certaines données, en retirant toute référence à la personne concernée, de manière à ce qu'elles ne constituent plus des données à caractère personnel au sens strict de la loi mais conservent néanmoins une utilité statistique (et donc une valeur économique pour l'entité les ayant collectées).

Cependant, plusieurs incidents se sont succédés depuis une quinzaine d'années, tels que l'affaire de la publication des requêtes des utilisateurs par AOL ou la ré-identification des clients de Netflix, qui remettent en cause l'effectivité même du principe de l'anonymisation de données, en démontrant en particulier que ce processus permet rarement de couper réellement le lien entre une personne et les informations qui la concerne. En pratique, il est très difficile d'évaluer le niveau d'anonymat offert par une méthode d'anonymisation particulière à l'aide d'une métrique suffisamment générique pour couvrir toutes les inférences qui pourraient être faites par un adversaire accédant à la version anonymisée des données. Globalement, l'anonymisation de données ne semble donc pas une réponse satisfaisante pour offrir une mise en place effective du droit à l'oubli.

3.2. Panorama des approches possibles

Tout informaticien est conscient que de par la nature numérique de l'information, il serait illusoire d'espérer pouvoir implémenter parfaitement le droit à l'oubli. En effet, une fois une donnée rendue publique, il est possible d'en faire très rapidement des milliers de copies et de les disséminer ensuite aux quatre coins de la toile. Ainsi, même si la donnée source est ensuite effacée, ainsi que toutes ses copies visibles, il restera toujours un doute sur l'existence éventuelle d'une copie non répertoriée. Néanmoins, il existe des solutions technologiques qui permettent de s'assurer qu'une donnée disparaîtra effectivement d'elle-même d'un système donné (indépendamment des copies qui ont pu en être faites), soit au bout d'un

[8] ANSSI, *Produits certifiés CC*, http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cc/
[9] ANSSI, *Produits certifiés CSPN*, http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/

certain temps soit sur demande d'une personne donnée. Ci-après, nous présentons un panorama de quelques unes des technologies qui nous semblent prometteuses en vue de permettre une implémentation (partielle et limitée) du droit à l'oubli.

3.2.1. Le principe des politiques adhésives

Une manière classique de définir les utilisations et opérations possibles pouvant êtres effectuées sur une donnée à l'intérieur d'un système d'information est de lui associer une politique de sécurité spécifiant les traitements qu'il est permis, interdit ou obligatoire d'effectuer avec la donnée en question. Les « politiques adhésives » (ou *sticky policies* en anglais)[10] poussent le concept encore plus loin en proposant de ne jamais séparer la donnée de la politique en question, même lorsque cette donnée devient mobile et est communiquée à travers un réseau informatique ou dans le cadre d'une application distribuée. Ainsi lorsqu'un fichier est transmis entre deux personnes, d'une machine à une autre ou entre différents programmes, la politique reste toujours associée à la donnée et lui est indissociable. Afin de s'assurer de l'application des politiques de sécurité, on peut être amené à s'appuyer sur certaines entités du système, dites « de confiance » et réputées respecter ces règles par hypothèse.

3.2.2. Publication éphémère de données

Le principe de la publication éphémère consiste à concevoir des systèmes informatiques dans lesquels toute donnée qui est insérée va finir par disparaître, sans pour cela requérir aucune action consciente de la part d'un utilisateur. Il est par exemple possible de créer un système de publication éphémère qui exploite à son avantage l'aspect dynamique de certains systèmes informatiques qui les rend ces derniers difficilement prédictibles, afin d'effacer petit à petit les données stockées dans le système. Vanish[11] est un système permettant à une donnée de disparaître automatiquement au bout d'un certain temps sans requérir aucune action explicite de la part du possesseur de cette donnée. En un certain sens, cette donnée peut donc être considérée comme étant dotée de capacités d'autodestruction.

3.2.3. Rendre une donnée introuvable

Une des raisons pour lesquelles il est très difficile de mettre en place le droit à l'oubli est ce que les moteurs de recherche tels que Google ou encore les agrégateurs de données comme 123People[12] sont devenus extrêmement compétents pour faire remonter toutes sortes de données liées à un individu, même si ces données sont dispersées dans les profondeurs du Web. Cependant, on peut considérer de la même manière qu'une donnée qui existe physiquement mais qui n'est pas indexée par ces moteurs de recherche (ou alors qui est retournée parmi les derniers résultats) peut être considérée comme ayant été « oubliée », car hors de portée de la plupart des internautes.

Ainsi, on peut par exemple rajouter dans le code HTML d'une page web un tag signifiant explicitement aux moteurs de recherche qu'on ne souhaite pas être référencé par ceux-ci. De plus, certaines entreprises de gestion de la réputation numérique proposent soit de jouer un rôle d'intermédiaire en demandant à une société hébergeant des données problématiques de les effacer, soit de noyer ces données sensibles sous des données « positives ». Pour l'instant, les approches visant à rendre une donnée introuvable en essayant de tromper les mécanismes de recherche semblent relever davantage de l'heuristique, n'offrant pas le type de garantie formelle qui permettrait d'établir avec une certitude mathématique des propriétés précises sur le devenir des données à oublier.

---

[10] G. Karjoth & M. Schunter, *A privacy policy model for enterprises.* In 15th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 2002.

[11] R. Geambasu, T. Kohno, A. A. Levy & H. M. Levy, *Vanish: Increasing data privacy with self-destructing data.* In Proceedings of the 18th USENIX Security Symposium, 2009.

[12] http://www.123people.com/