BANQUE DES MEMOIRES

Master de droits de l'homme et droit humanitaire
Dirigé par Emmanuel Decaux
2011

Le droit à l'oubli numérique sur les réseaux sociaux

Etienne Quillet

Sous la direction de Emmanuel Decaux

Remerciements

Je tiens à remercier Monsieur Decaux d'avoir accepté de prendre ce mémoire sous sa direction et d'en avoir proposé la publication, ainsi que toute l'équipe enseignante du Master de droits de l'homme et droits humanitaire pour leurs conseils avisés et la richesse de leurs enseignements.

Mes remerciements vont également à Jérôme Benzimra-Hazan pour son soutien et l'intérêt qu'il a porté à mes recherches.

SOMMAIRE

INTRODUCTION

Préambule

La récente réflexion qui s'est installée en France et en Europe sur l'existence et la consécration d'un « droit à l'oubli numérique » en droit positif peut paraître surprenante. Il paraît contestable qu'un phénomène psychique tel que l'oubli, souvent considéré comme destructeur en ce qu'il s'oppose aux vertus de la mémoire, puisse être appréhendé par le droit de manière substantielle.

En réalité, l'oubli peut être vu de manière positive, comme une sorte de « mal nécessaire ». Mais surtout, les revendications d'un « droit à l'oubli » répondent à l'explosion des technologies numériques, qui exposent désormais tout individu à la conservation intemporelle de ses souvenirs.

Ce d'autant plus qu'avec le développement de l'Internet, l'homme est amené à laisser à son sujet, à tout âge, à tout instant de sa vie, quantité de données et de traces le concernant directement, ou indirectement. Les réseaux sociaux à ce titre, semblent parfaitement cristalliser les enjeux qui existent aujourd'hui autour du « droit à l'oubli numérique », tant ils révèlent à la fois l'importance de « l'oubli », mais aussi les inévitables obstacles théoriques et techniques que rencontre sa mise en œuvre.

Approche ontologique de l'oubli

Le terme d'« oubli » renvoie à deux phénomènes bien distincts. Dans un sens positif, il correspond à l'action ou la faculté d'oublier. Dans un sens négatif au contraire, il renvoie à l'échec de la mémoire, à la perte du souvenir.

On a souvent tendance à privilégier cette dernière approche, en portant sur l'oubli un regard réprobateur. Ainsi, l'oubli est notamment considéré comme un obstacle à l'exercice du devoir de mémoire[1]. L'exemple le plus frappant est celui de la Shoah. Au lendemain de la Seconde Guerre mondiale, un constat s'impose : « Plus jamais ça ! ». Les générations présentes et futures *doivent* savoir. Elles ont le *devoir* de se souvenir, afin d'éviter que ne se reproduise une telle tragédie. Par opposition au devoir de mémoire, l'oubli est dans ce cas vu comme un fléau, comme un « mal » à combattre.

L'oubli peut aussi être perçu comme une faiblesse. Il est alors ce qui empêche l'individu de se souvenir. Il renvoie à l'idée de défaillance de la mémoire, en ce qu'il constituerait un obstacle à l'accès et à la conservation des connaissances.

Enfin, l'oubli est parfois assimilé à une certaine forme de dégénérescence, notamment dans le cadre des maladies neurodégénératives qui touchent les personnes âgées et entraînent la perte progressive des fonctions mémorielles, telle la maladie d'Alzheimer. Dans ce cas, oublier « c'est s'approcher de la mort[2] ».

Selon ces différentes perspectives, l'oubli ne serait qu'une résultante négative de la mémoire. En d'autres termes il ne serait qu'une sorte de « mémoire en défaut[3] ». Mais l'oubli, dans une perspective individuelle, peut être envisagé de manière positive, en tant que phénomène *en soi*, voire en tant que nécessité. A ce titre, il doit être appréhendé comme une puissance créatrice, au même titre que la mémoire.

---

[1] Voir sur le sujet les ouvrages de Paul RICOEUR, notamment : *La mémoire, l'histoire, l'oubli*, Le Seuil, 2000.

[2] Christine KOSSAIFI: « L'oubli peut-il être bénéfique ? L'exemple du mythe de Léthé : une fine intuition des Grecs » *Revue pluridisciplinaire en sciences de l'homme et de la société ¿ Interrogations ? Numéro 3. L'oubli*. Décembre 2006. Source http://www.revue-interrogations.org/fichiers/57/mythe_de_lethe.pdf.

[3] L'oubli, Appel à contribution. ¿Interrogations ? - *Revue pluridisciplinaire en sciences de l'homme et de la société. Numéro 3. L'oubli*. Décembre 2006. Préface par le comité de rédaction. Source : http://www.revue-interrogations.org/fichiers/contrib6/Appel%20a%20contribution%203%20l%20oubli.pdf.

On trouve dans la littérature philosophique et scientifique différentes approches positives de l'oubli. Pour Nietzsche par exemple, l'oubli est essentiel au développement de la personne humaine. Il agirait comme une force de digestion face aux évènements qui interviennent dans une vie. Il serait ainsi une « faculté active […] chargée de maintenir l'ordre psychique, la tranquillité[4] ». L'oubli serait même la condition du bonheur : « Nul bonheur, nulle sérénité, nulle espérance, nulle fierté, nulle jouissance de l'instant présent ne pourrait exister sans faculté d'oubli[5] ». Autrement dit, la possibilité d'oublier correspond pour Nietzche, *in fine,* à « la faculté de se sentir pour un temps en dehors de l'histoire[6] ».

La psychanalyse perçoit quant à elle l'oubli comme un principe de frustration. L'oubli serait l'action positive – bien qu'inconsciente – qui consiste, non pas en une perte, mais en un refoulement du souvenir[7].

Enfin, dans une perspective bergsonienne, on pourrait envisager l'oubli comme la part variable de la conscience. En effet pour Bergson, « la conscience signifie d'abord mémoire[8] ». Par conséquent, ce que l'oubli retirerait à la mémoire déterminerait l'état de conscience d'un individu à un moment donné. L'oubli interviendrait alors, selon les termes de Nietzsche, pour « fermer de temps en temps les portes et les fenêtres de la conscience[9] ».

L'expression – non exhaustive – de ces courants de pensée met en lumière le rôle fondamental de l'oubli dans le développement de la personne humaine. L'homme effectue en lui-même un arbitrage permanent entre la mémoire et l'oubli. C'est une constante inhérente au psychisme de l'homme. C'est un équilibre naturel.

L'homme dispose de nombreux outils qui lui permettent de se souvenir. Il a toujours laissé autour de lui de nombreuses traces (dans la mémoire des hommes, par un écrit, une peinture, un objet, etc). Ces traces, jusqu'à une époque récente, se fixaient sur un support matériel. Ce support pouvait s'altérer, il pouvait se perdre. Il n'était pas forcément

---

[4] NIETZSCHE *Considérations intempestives*, II, 1, 1874 tr. fr. G. Bianquis, éd. Aubier-Montaigne.

[5] *Ibid*.

[6] *Ibid*.

[7] Voir par exemple FREUD, « Psychonévroses de défense », in *Névrose, Psychose et Perversion*, Paris, P.U.F.

[8] Henri BERGSON : *L'Energie spirituelle. Essaiset conférences* (1919), P.U.F., 2009, Chapitre I, p.34.

[9] NIETZSCHE, *Généalogie de la morale,* Flammarion, 1996.

reproductible. Par ailleurs, il ne pouvait être que ponctuel : il était quasiment impossible de conserver sur un support matériel chaque instant de la vie de chaque individu. On ne disposait pas à cet effet d'une capacité de stockage et d'archivage suffisante. Cela pouvait en outre s'avérer particulièrement coûteux. Dès lors, nécessairement, toute chose tombait plus facilement dans l'oubli qu'elle ne se conservait. Pour reprendre les mots de M. Bensoussan, auparavant « les relations disparaissaient, les écrits jaunissaient, et l'histoire disparaissait[10] ».

L'oubli à l'ère numérique

Le développement récent des technologiques numériques et informatiques vient cependant bouleverser cet équilibre. Viktor Mayer Schönberger dans un ouvrage remarqué sur les « vertus de l'oubli à l'ère numérique[11] », identifie quatre évolutions déterminantes.

La première est le développement de la technologie numérique (ou digitalisation). Elle a selon lui donné naissance à une nouvelle génération de traitement, de stockage, de récupération et de partage de l'information, sensiblement supérieure à ce que permettait la technologie analogique. Elle permet désormais la reproduction fidèle d'une information, avec une qualité inaltérable, et en n'utilisant qu'un seul et même support, quel que soit l'opération ou le type d'information en cause.

La deuxième évolution qu'il identifie est la baisse considérable des coûts de stockage de l'information sous format numérique pour les consommateurs, et pour les fournisseurs de service. Chacun peut aujourd'hui conserver une trace de sa vie et de ses moindres pensées pour un coût relativement faible. La conséquence est alors une augmentation du coût de « l'oubli » : plus le volume d'information qui peut être conservé est important, plus il devient coûteux de trier et choisir l'information que l'on veut conserver et celle que l'on souhaite supprimer.

[10] Propos tenus lors de la conférence sur le droit à l'oubli numérique à Sciences-Po Paris, organisée le jeudi 12 novembre 2009 par Nathalie Kosciusko-Morizet, alors secrétaire d'État en charge de la prospective et du développement de d'économie numérique.

[11] V.MAYER SCHÖNBERGER : *Delete: The virtue of forgetting in the digital age*, 2009, Princeton university press, 237 p.

En troisième lieu, l'avènement d'outils de recherche bon marché, répandus et simples à utiliser (tels que les moteurs de recherche, ou les logiciels d'indexation), rend l'accès à l'information extrêmement facile, en tout temps et en tout lieu.

Enfin, la globalisation des réseaux numériques a éliminé la contrainte de la présence physique à l'endroit où l'information que l'on veut atteindre est stockée. Aujourd'hui, une simple connexion au réseau suffit pour accéder à une donnée.

Cette « révolution numérique », selon l'expression consacrée, en permettant l'avènement d'une mémoire numérique parfaite, a opéré un renversement de l'équilibre mémoire/oubli. Ainsi que l'écrit V.M. Schönberger, elle a « fondamentalement bouleversé le type d'information dont il est possible de se souvenir, la manière dont on s'en souvient, et à quel coût […]. De manière évidente, le souvenir est devenu la norme, et l'oubli l'exception[12] ».

Ce changement de paradigme n'est pas forcément néfaste en soi. En effet, il n'a pas pour conséquence de priver l'homme de sa faculté d'oublier. En revanche, il l'expose à une conservation intemporelle de toute trace qu'il laisserait dans la mémoire numérique et, partant, à la résurgence intempestive et dommageable d'une information qui était tombée dans l'oubli. Autrement dit, la révolution numérique n'a pas altéré le *mécanisme* de l'oubli, mais plutôt *l'effectivité* de l'oubli. Ce qui est préoccupant, ce sont donc les conséquences qui peuvent découler de ce décalage entre le passé vécu, ou ressenti, et le passé numérique : si le passé dont nous nous souvenons change et évolue sans cesse, celui inscrit dans la mémoire numérique est figé dans le temps.

Ce décalage est encore accentué avec le développement de l'Internet. Ce dernier, bien qu'il constitue un vecteur évident de communication et de liberté[13], fait de chaque individu un véritable fournisseur d'informations. En effet, l'internaute laisse sur la « Toile » de nombreuses « traces[14] ». Celles-ci permettent, grâce au développement

[12] *Ibid*, p.52. Citation originale : « Modern technology has fundamentally altered what information can be remembered, how it is remembered, and at what cost […] Quite obviously, remembering has become the norm, and forgetting the exception ».

[13] A ce sujet, voir par exemple le rapport de Frank LA RUE, rapporteur des Nations-Unies pour la promotion et la protection de droit à la liberté d'opinion et d'expression, A/HRC/17/27.

[14] On distingue d'ordinaire les traces volontaires des traces involontaires. Une trace volontaire correspond à toute donnée publiée délibérément par l'internaute (article, commentaire, identité, etc.). Une trace involontaire constitue en revanche une donnée récoltée lors de la navigation. Il peut s'agir d'une adresse IP,

d'algorithmes puissants, de dresser un profil de plus en plus précis de l'internaute. Le problème est que cette information n'est pas neutre. Bien au contraire, elle a une valeur marchande. Car au-delà de la question de l'accès à Internet, l'utilisation d'un service sur la Toile n'est pas « gratuite ». L'internaute est en réalité un « consommateur », qui recourt à divers « services ». Et ces services doivent être rémunérés. Or, il est désormais notoire que les fournisseurs de services sur internet (sites, moteurs de recherche, réseaux sociaux, etc.) se financent grâce aux revenus publicitaires. Ils ont donc intérêt à récolter une information la plus complète possible, afin de pouvoir établir un profil précis de l'internaute. De ce profil, les régies publicitaires déduisent la publicité la mieux adaptée au consommateur. Ainsi, l'information devient « la matière première du monde économique[15] ».

Par ailleurs, le foisonnement des informations, leur accessibilité par tous en tout temps et en tout lieu, et leur durabilité potentiellement illimitée, ont engendré un transfert du pouvoir sur l'information, du sujet, au récepteur. En d'autres termes, dès lors que certains (fournisseurs de service, particuliers, etc.) ont accès à des données nous concernant, nous perdons le pouvoir et le contrôle sur celles-ci. Il en résulte une destruction du rapport de l'homme à la notion de pouvoir, mais aussi à la notion de temps : la perte du pouvoir sur l'information entraîne un ancrage potentiellement permanent du « souvenir numérique » dans la mémoire numérique et, partant, une modification du rapport de l'homme au temps. Ainsi, pour V.M. Schönberger, la révolution numérique menacerait notre capacité à mettre les évènements en perspective dans le temps et à décider de manière rationnelle. Elle pourrait aussi confronter l'homme à une contradiction entre le souvenir « humain » et le « souvenir numérique ». Il est donc à craindre que, irrémédiablement attachés à notre passé numérique, nous perdions confiance en nos propres souvenirs et arrêtions de croire au passé *tel que nous nous en souvenons*.

C'est dans ce contexte qu'a été revendiquée la reconnaissance juridique d'un « droit à l'oubli numérique », dont s'est fait écho le Tribunal de grande instance de Paris, sous la plume de son vice-président, Joël Boyer[16] . La formule mérite d'être reproduite telle

---

des mots-clés saisis dans un moteur de recherche, de cookies, de l'historique et de la fréquence des sites visités, etc.

[15] A. BELLEIL *: E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'Internet, Dunod*, 2001, p.11.

[16] Tribunal de Grande instance de Paris (Ord. Réf) 25 juin 2009, *Vernes c. SAS les Échos*, Légipresse, no. 266, novembre 2009, p. 215 (Note MALLET-POUJOL).

qu'elle, tant elle exprime de manière limpide le contexte et les enjeux de la reconnaissance d'un tel droit :

> *« Si l'oubli procédait jadis des faiblesses de la mémoire humaine, de sorte qu'il n'y avait pas à consacrer un droit à l'oubli, la nature y pourvoyant, la société numérique, la libre accessibilité des informations sur internet, et les capacités sans limites des moteurs de recherche changent considérablement la donne et justifie pleinement qu'un tel droit soit aujourd'hui revendiqué, non comme un privilège qui s'opposerait à la liberté d'information, mais comme un droit humain élémentaire à l'heure de la société de conservation et d'archivage numérique sans limite de toute donnée personnelle et de l'accessibilité immédiate et globalisée à l'information qui caractérisent les technologies contemporaines et la fascinante insouciance qu'elles suscitent ».*

La nature du « droit à l'oubli numérique »

D'après Roseline Letteron, l'expression « droit à l'oubli » aurait été forgée en 1966 par le professeur Gérard Lyon-Caen[17]. A cette époque, le « droit à l'oubli » revêtait une signification bien particulière. Il renvoyait à un « oubli » décidé, ou imposé de l'extérieur, au moyen d'une norme impérative, afin de garantir la paix et la cohésion sociale. Les lois d'amnistie, les règles relatives à la prescription, ou encore l'interdiction de mentionner les condamnations ayant fait l'objet d'une réhabilitation, illustrent bien cette approche. Tout fait prescrit, ou tout fait ayant fait l'objet d'une amnistie, ne peuvent donner lieu à aucune poursuite, ni à aucune condamnation. Ainsi, le choix des délais de prescription, ou le choix de l'amnistie, semblent relever davantage d'un choix de société, ou d'une question d'ordre public, que de la protection d'un droit de la personne. Le « droit à l'oubli », entendu comme droit au respect de ces normes, est donc un droit à dominante objective[18].

---

[17] T.G.I., Seine, 14 octobre 1965, *Mme Segret c. Soc. Rome-Paris Films*, note de GERARD LYON-CAEN, J.C.P, 1966.II.14482. Cité par ROSELINE LETTERON « Le droit à l'oubli », Revue du droit public, 1996, T. CV, n°2, p. 388 note 15.

[18] Un temps reconnu par des juges de première instance (T.G.I. Paris, 20 avril 1983, *Mme Filipacchi* et soc. Cogedipresse), le « droit à l'oubli » en tant que droit subjectif a finalement été écarté par la Cour de

On assiste cependant, avec la révolution numérique, à un renversement de perspective. Le « droit à l'oubli », en tant que droit subjectif, est unanimement revendiqué en tant que droit fondamental de la personne humaine[19]. Sa définition fait toutefois l'objet de nombreuses interprétations différentes. Pour certains, il s'agirait d'un « droit d'être laissé tranquille[20] », ou d'un « droit à l'intimité ». Le droit à l'oubli serait alors une conséquence du droit au respect de la vie privée. Pour d'autre, le droit à l'oubli se rapprocherait d'un « droit à l'autodétermination informationnelle[21] ». Il s'agirait de conférer à la personne le pouvoir de décider elle-même la mesure dans laquelle les informations la concernant peuvent être traitées, communiquées, et conservées. Par analogie, le droit à l'oubli serait donc le droit de décider soi-même quelles informations nous concernant doivent tomber dans l'« oubli ». Toutefois, ce droit semble devoir être entendu dans un sens plus restreint que le « droit à l'autodétermination informationnelle », qui implique en effet une maîtrise générale de l'information. En effet, le droit à l'oubli, dans un sens strict, ne vise que la maîtrise de l' « oubli », c'est-à-dire la disparition ou non du « souvenir ».

La diversité de ces approches semble due à l'ambigüité de l'expression « droit à l'oubli ». En effet, « l'oubli » se situe sur deux plans distincts. Il s'agit d'une part de l'oubli qui s'opère sur le plan psychique (la disparition du souvenir), et d'autre part de l'oubli qui s'opère sur le plan numérique (la disparition de l'information). Or, ainsi que l'écrivait Roseline Letteron, le droit ne peut pas appréhender de manière substantielle l'oubli en tant que réalité psychique. Autrement dit, « l'oubli » est envisagé en tant que *fiction*[22]. Il ne peut appréhender qu'une réalité tangible. Ainsi le droit à « l'oubli » ne vise

---

cassation, qui a estimé que la maîtresse d'un ancien collaborateur « ne pouvait se prévaloir d'un droit à l'oubli » pour empêcher qu'il soit fait état de son passé dans un livre publié en 1986 (Cass. Civ. 1re, 20 novembre 1990, *Mme Monanges c. Kern*).

[19] Rapport n° 72 (1977-1978) de M. Jacques THYRAUD, fait au nom de la commission des lois, déposé le 10 novembre 1977.

[20] A. BELLEIL, op.cit., p. 2.

[21] Ce droit a fait l'objet de nombreux développements, notamment de la part d'Yves POULLET et d'Antoinette ROUVROY, à la suite d'un arrêt venu consacrer ce droit, rendu par la Cour Constitutionnelle fédérale allemande (Bundesverfassungsgerichsthof) du 15 décembre 1983 (BVGE 65, 1.). Voir également Y. POULLET, J.-M. DINANT, avec la collaboration. de C. de TERWANGNE ET M.-V. PEREZ-ASINARI : « L'autodétermination informationnelle à l'ère de l'Internet », Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

[22] Roseline LETTERON « Le droit à l'oubli », *Revue du droit public*, 1996, T. CV, n°2, p.

directement que le souvenir « numérique », c'est-à-dire l'information concernant une personne identifiée ou identifiable, qui est conservée dans la mémoire numérique. Pour cette raison, il semble préférable de recourir à l'expression « droit à l'oubli numérique ».

En définitive, le droit à l'oubli numérique, dont la finalité est la protection de la personne contre l'intangibilité de son passé, correspond au pouvoir qu'un individu devrait avoir sur l'existence ou la disparition d'une information le concernant. C'est donc le droit de l'internaute à la disparition de ses « souvenirs numériques ».

L'« oubli numérique » sur les réseaux sociaux

Le « droit à l'oubli numérique » mérite d'être étudié à l'aune de tous les espaces de communications qu'offre l'Internet. Les réseaux sociaux, aujourd'hui, en sont l'un des principaux. Ces derniers sont l'une des innovations les plus caractéristiques du « web 2.0[23] ». Ils se sont développés de manière extrêmement rapide ces dernières années, tant par l'apparition de nouveaux réseaux, que par l'accroissement considérable du nombre de leurs membres.

Ils peuvent recouvrir des réalités très diverses. Le groupe de l'article 29[24] (ci-après le « G29 ») a proposé dans un avis de 2009 de définir ces « services de réseautage social » (ci-après « SRS »), comme « des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs[25] ». Le groupe de travail a par ailleurs identifié quatre caractéristiques communes à ces réseaux. En premier lieu, les utilisateurs sont invités à fournir des données à caractère personnel permettant de constituer un « profil ». Ensuite, les SRS mettent à la disposition de leurs

[23] Le Web 2.0, dit aussi « web social » est le terme utilisé pour décrire l'ensemble des fonctionnalités et des techniques qui ont succédé à l'Internet dans sa forme initiale. Le Web 2.0 est plus simple et plus accessible. Il offre un réseau non plus statique, mais dynamique. L'internaute autrement dit, ne se borne plus à rechercher l'accès à une information, il peut également en créer, et en partager.

[24] Le groupe de travail «article 29» sur la protection des données a été institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il a un caractère consultatif et agit en toute indépendance. Ses avis sont souvent pris comme référence, et sont largement relayés par les autorités de protection des données à l'échelle européenne, et notamment par la CNIL.

[25] Voir l'avis du G29, WP 163, Avis 5/2009 sur les réseaux sociaux en ligne adopte le 5 juin 2009.

membres des outils leur permettant de mettre leur propre contenu en ligne (tel que des photos, des commentaires, de la musique, des vidéos ou des liens vers d'autres sites, etc.). Chaque membre a par ailleurs à sa disposition une liste de contacts avec lesquels il peut interagir. Enfin, les SRS se financent grâce aux revenus de la publicité diffusée sur les pages web auxquelles les utilisateurs accèdent. Les informations fournies par ces derniers permettent ainsi de dresser d'eux un « profil » sur la base duquel ils sont ciblés, le cas échéant, par différentes régies publicitaires. Le succès d'un réseau dépend alors en partie de la quantité d'informations fournie par ses membres.

Les réseaux sociaux offrent des fonctionnalités diverses, et poursuivent des finalités diverses. Ils peuvent avoir une finalité purement sociale (Facebook, MySpace, Google+, etc.), ou bien une finalité spécifique. Ainsi, les réseaux LinkedIn et Viadeo ont par exemple vocation à créer des réseaux professionnels. D'autres, tel le réseau Copainsdavant, permettent à leurs membres de retrouver d'anciens camarades qui ont partagé leur scolarité, ainsi que leurs activités associatives et professionnelles.

En principe, un internaute publiant une information sur de tels réseaux est censé être responsable. Les informations qu'il y publie sont en effet volontaires, et relèveraient donc de sa responsabilité. D'ailleurs, les réseaux sociaux invoquent généralement l'argument selon lequel un membre présent sur le réseau est averti des modalités de publication et d'utilisation de ses données, par le biais des « Conditions générales d'utilisations », qu'il doit avoir acceptées lors de son inscription. L'utilisateur pourrait également, grâce aux « paramètres de confidentialité », restreindre l'accès aux informations qu'il publie à ses contacts. Enfin l'utilisateur est censé être conscient et raisonnable, puisqu'il est en théorie interdit de s'inscrire en-deçà d'un certain âge (13 ans minimum sur Facebook par exemple). En pratique cependant, on s'aperçoit que les « Conditions générales d'utilisation » sont parfois peu lisibles, et que les paramètres de confidentialité sont souvent ouverts par défaut à tous les utilisateurs (tous les membres ne font pas la démarche, sciemment ou non, de restreindre leurs « profils »). Quant aux limites d'âges imposées, de nombreuses études ont mis en lumière la présence de plus en plus

importante de très jeunes adolescents sur les réseaux sociaux, qui ne renseignent pas leur âge véritable lors de l'inscription[26].

Par ailleurs, de nombreuses études révèlent que les informations publiées par les utilisateurs peuvent être accessibles à des personnes non membres du réseau. Ainsi, on constate une pratique croissante des cabinets de recrutement à consulter le profil de leurs potentiels futurs employés, ou encore la consultation par les employeurs du profil de leurs salariés. La presse à ce titre ne manque pas de se faire écho des personnes licenciées, ou non embauchées, sur la base du contenu qu'elles avaient mis en ligne. Un exemple, qui fait désormais figure de symbole est celui de Stacy Snyder. Cette élève enseignante, s'était vue reprocher d'avoir mis sur internet une photo d'elle coiffée d'un chapeau de pirate et portant à sa bouche un gobelet en plastique, qu'elle avait elle-même intitulée « Pirate Ivre ». Considérant cette conduite « non-professionnelle », son université, en 2006, avait refusé de lui délivrer son diplôme. Elle avait alors voulu supprimer la photo du site internet mais en vain : la page internet avait déjà été cataloguée et la photo archivée par divers moteurs de recherche. Quoiqu'elle fasse, le « souvenir numérique » de sa soirée était définitivement figé dans la mémoire de la « Toile ».

Ainsi, les réseaux sociaux constituent à l'heure actuelle un laboratoire privilégié de l'existence et de la mise en œuvre d'un « droit à l'oubli numérique ». La quantité considérable d'informations publiées, leur accessibilité, et leur potentiel de diffusion, pose avec une acuité toute particulière la question de leur conservation, et de la maîtrise que peut avoir sur elles leur sujet.

L'enjeu de la présente étude sera donc de déterminer la mesure dans laquelle une personne maîtrise l'existence d'un « souvenir numérique » la concernant sur un réseau social. D'un point de vue juridique, cela revient à se demander si l'existence éventuelle de ce pouvoir se traduit concrètement par l'existence d'un droit.

[26] Selon une étude réalisée en 2011 par TNS SOFFRES pour le compte de la CNIL, près de 20% des moins de 13 ans ont un compte 48% des enfants de 8-17 ans sont connectés à un réseau social (Facebook). http://www.cnil.fr/la-cnil/actu-cnil/article/article/reseaux-sociaux-quelles-sont-les-pratiques-de-nos-enfants-quel-est-le-role-des-parents/?tx_ttnews[backPid]=2&cHash=66639ddc7d.

Il s'agira autrement dit de répondre à la question suivante : existe-t-il un « droit à l'oubli numérique » permettant à toute personne de maîtriser dans le temps et dans l'espace l'information qui la concerne sur un réseau social ? Et dans quelle mesure ce droit est-il applicable, et appliqué ?

Seront recherchées, dans un premier temps, les règles de droit positif, notamment celles relatives à la protection des données, témoignant de l'existence d'un droit à « l'oubli numérique » permettant à l'individu de maîtriser la vie de ses « souvenirs numériques ». On se concentrera essentiellement sur la législation européenne, et plus particulièrement sur la législation française qui l'a transposée, qui sont à l'heure actuelle les plus abouties en matière de protection des données. La démonstration tendra à vérifier l'hypothèse selon laquelle ce droit existe, bien que de manière implicite, et qu'il est potentiellement applicable sur les réseaux sociaux (Première Partie).

Dans un deuxième temps, la réalité de ce droit sera confrontée à la pratique et aux incertitudes juridiques qu'il suscite. Des propositions seront alors développées pour une meilleure effectivité du « droit à l'oubli numérique » sur les réseaux sociaux (Deuxième Partie).

PREMIERE PARTIE : L'IDENTIFICATION D'UN DROIT A L'OUBLI NUMERIQUE APPLICABLE AUX RESEAUX SOCIAUX

Le droit à l'oubli numérique, en droit positif, peut être trouvé dans plusieurs textes, à l'échelle européenne et nationale (I). Ces textes sont la Convention n°108 du Conseil de l'Europe[27], les directives 95/46/CE, 2002/58/CE du Parlement européen et du Conseil de l'Union européenne[28] et, en France, la Loi du 6 Janvier 1978, dite aussi loi « Informatique et Libertés[29] ». Cette existence constatée, il est alors possible d'envisager, de manière extensive, selon quelles modalités il pourrait être mis en œuvre (II).

I. L'existence du droit à l'oubli numérique en droit positif

S'il s'agit de déterminer précisément, à l'aune du droit positif, le contenu du droit à l'oubli numérique, il est aussi nécessaire d'en déterminer le contour, ou les limites. Car le droit à l'oubli numérique ne saurait être exercé au détriment d'autres droits, tel par exemple le droit à la liberté d'expression. L'identification du droit à l'oubli passe donc par une démarche en deux temps, préconisée notamment par Alain Bensoussan[30], qui vise à explorer le cœur du droit (A), et à en déterminer les frontières (B).

---

[27] Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, STCE n° 108, entrée en vigueur le 05/10/1985.

[28] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050 ; Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) Journal officiel n° L 201 du 31/07/2002 p. 0037 – 0047 ; Charte des droits fondamentaux de l'Union européenne (2000/C 364/01).

[29] Loi n°78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés (ci-après loi « Informatique et Libertés »* (modifiée notamment par la loi n°2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel portant transposition de la directive 95/46/CE*).

[30] Propos tenus lors de la conférence sur le droit à l'oubli numérique à Sciences-Po Paris, organisée le jeudi 12 novembre 2009 par Nathalie Kosciusko-Morizet, alors secrétaire d'État en charge de la prospective et du développement de d'économie numérique.

A. Le cœur du droit à l'oubli numérique

Les législations française et européenne, sans pour autant mentionner expressément le droit à l'oubli numérique, comportent des dispositions qui permettent à un individu, selon certaines modalités, et sous certaines conditions, de maîtriser l'existence des informations le concernant. L'identification de ces dispositions permet de préciser le contenu du droit à l'oubli numérique (1). En revanche, la référence explicite au droit à l'oubli numérique n'est encore qu'à l'état de projet, ou de « droit mou » dans les législations françaises et européennes (2).

1. Le contenu du droit à l'oubli numérique en droit positif

Le droit à l'oubli numérique suppose l'identification de l'objet de l'« oubli ». Nous avons proposé à cet effet le terme générique de « souvenir numérique ». Il convient alors de rechercher la traduction juridique de ce « souvenir ». En l'état actuel du droit, il s'agit d'une « donnée à caractère personnel » faisant l'objet d'un « traitement » (a). Dans ce cadre, l'individu dispose de certains droits, qui constituent l'essence du droit à l'oubli numérique (b).

a. Identification juridique du « souvenir numérique : une « donnée à caractère personnel » faisant l'objet d'un « traitement »

Les droits dont on verra qu'ils constituent le cœur du droit à l'oubli ne peuvent être mis en œuvre que s'ils s'inscrivent, aux termes des diverses législations relatives à la protection des données, dans le cadre d'un « traitement de données à caractère personnel[31] ».

Les « données à caractère personnel ». Aux termes de l'article 2. a). de la directive 95/46/CE, une donnée à caractère personnel peut être définie comme « toute information concernant une personne physique identifiée ou identifiable ». De manière générale, l'identification passe par la connaissance de l'identité civile de la personne, au

[31] Article 3 de la Convention n°108 du Conseil de l'Europe ; article 3 directive 95/46/CE ; Article 3 directive 2002/58/CE ; article 2 loi « Informatique et Libertés ».

moyen de données précises, tel que le nom, le prénom, et la date de naissance. Ce sont ces données qui, selon la Directive, renvoient à une personne physique « identifié ». Le terme « identifiable » suggère cependant que la notion de données personnelles doit être entendue dans un sens large. En effet, la possibilité d'identifier une personne n'implique plus nécessairement de connaître son identité civile. Elle est notamment rendue possible par le développement des techniques de « désanonymisation[32] », ou par l'analyse des traces laissées sur le web[33] au moyen d'algorithmes permettant de mettre en relation la multitude des informations collectées. La directive, en son considérant 26, suggère néanmoins une approche « raisonnable » pour déterminer si une personne est identifiable. Selon le G29, cela signifie que si, compte tenu des moyens susceptibles d'être raisonnablement mis œuvre, la possibilité d'identifier une personne n'existe pas ou est négligeable, ladite personne ne devra dès lors pas être considérée comme identifiable et les informations concernées ne devront pas être qualifiées de données à caractère personnel[34].

La Loi du 6 janvier 1978 modifiée, en son article 2§2, reprend en substance la définition de la directive. Elle ne reprend cependant pas le critère de l'approche « raisonnable ». Tous les moyens techniques permettant de déterminer si la personne est identifiable ou non devraient donc être pris en compte.

Il ne s'agit pas ici de rentrer dans le vaste débat de savoir ce qui est, ou ce qui n'est pas une donnée à caractère personnel[35]. On retiendra seulement que la notion de donnée à

---

[32] La « désanonymisation » est un terme technique qui renvoie par opposition à l'anonymisation des données. L'anonymisation permet de rendre théoriquement impossible le rapprochement entre une donnée et la personne qu'elle concerne. Cela est rendu possible notamment grâce l'utilisation de techniques de cryptage et l'utilisation de clés de hachage. La « désanonymisation » est donc le procédé visant à rétablir la correspondance initiale à la personne et l'information. Cela peut se faire par exemple en brisant les clés de hachage utilisées, ou en procédant par recoupements à l'aide d'autres informations. Voir cependant, pour une étude révélant les limites de la désanonymisation : « Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy » Cavoukian, Ann et Eman, Khaled El. Information and Privacy Commissioner, Ontario, Canada, June 2011, 19 pp. Disponible à l'adresse : http://www.ipc.on.ca/images/Resources/anonymization.pdf.

[33] Voir en ce sens l'avis 4/2007 du G29 sur le concept de données à caractère personnel 01248/07/FR, WP 136, adopté le 20 juin 2007.

[34] *Ibid.*

[35] Outre l'identification au cas par cas de ce qui constitue, ou non, une donnée à caractère personnel », il existe un débat aujourd'hui sur l'existence même de ce genre de données. Certains estiment en effet que les nouvelles technologiques de stockage, de diffusion et de recoupement des informations font de toute « trace » une donnée à caractère personnel. On observerait selon eux un basculement vers le « tout donnée personnelle ». Au contraire, d'autres estiment que le web est désormais devenu un espace public et « désanonymisé », et que par conséquent, une donnée ne peut être que publique et non personnelle.

caractère personnel a potentiellement un champ extrêmement étendu en droit français, et qu'il s'agit d'une notion évolutive.

Les données dites « sensibles ». Il s'agit d'une catégorie particulière de donnée à caractère personnel. Elles sont définies comme toute « donnée à caractère personnel qui [fait] apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci[36] ».

Le « traitement ». Ces données doivent faire l'objet d'un « traitement ». Selon l'article 2§3 de la loi « Informatique et Libertés », constitue un traitement de données à caractère personnel « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction[37] ». Le terme « notamment » indique que la liste n'est pas limitative. Dès lors, de manière générale, le traitement correspond donc à la manipulation d'une donnée à caractère personnel, sensible ou non.

Le traitement, lorsqu'il n'est pas expressément interdit, est soumis à de nombreuses formalités (tels les mécanismes d'autorisation et de déclarations) et à de nombreuses conditions. La licéité du traitement obéit à des exigences de « loyauté », de « légitimité », de « pertinence » et de « proportionnalité ». On voit, ainsi que l'écrivait M. Decaux en 2009, que « tout est matière d'interprétation[38] ». De telles dispositions, ne nécessitent pas une analyse approfondie dans le cadre de l'étude du droit à l'oubli numérique. En effet, leur respect n'est pas une condition de mise en œuvre de ce dernier : il est invocable dès

[36] Article 8. I. de la loi « Informatique et Libertés ». Voir aussi : article 6 de la Convention n°108 du Conseil de l'Europe ; article 8.1. de la directive 95/46/CE.

[37] Voir aussi : article 2. c. de la Convention n°108 du Conseil de l'Europe (qui parle plutôt de « traitement automatisé) ; article 2.b. de la directive 95/46/CE.

[38] Emmanuel DECAUX : « La protection de la vie privée au regard des données informatiques », *Revue électronique Droits fondamentaux*, n° 7, janvier 2008 – décembre 2009, p.3.

lors qu'un tel traitement existe, qu'il ait été mis en œuvre licitement (respectant toutes les prescriptions imposées par la loi) ou en violation de la Loi du 6 janvier 1978.

b. Les droits constituant le droit à l'oubli numérique

Selon que le droit à l'oubli numérique est défini dans un sens étroit, ou dans un sens large, les droits qui le constituent varient.

Le droit à l'oubli numérique *latto sensu*. Dans un sens large, le droit à l'oubli s'entend comme le droit à la maîtrise de toute donnée à caractère personnel. Il se matérialiserait par une durée limitée de conservation des données, par le droit à l'information de leur sujet, le droit d'accès, le droit de rectification et de suppression, et par le droit d'opposition[39]. Autrement dit, il s'agirait, tout au long de la vie du « souvenir numérique » de garder la maîtrise de celui-ci, afin de pouvoir disposer, en temps voulu, de sa disparition complète et effective. Le droit à l'oubli numérique ne serait alors qu'un terme générique sous la bannière duquel seraient portés tous les droits inscrits dans la loi « Informatique et Libertés » qui permettent à l'individu d'agir sur la conservation, la teneur, et la diffusion de ses données personnelles.

La volonté d'élargir la compréhension du droit à l'oubli numérique est valable à de nombreux égards. Elle tient notamment compte des contraintes structurelles et techniques de l'Internet. En effet, la disparition d'une donnée serait difficile dès lors qu'elle aurait été diffusée, conservée et utilisée à de nombreux endroits et par de nombreuses personnes différentes. L'ambition d'un tel droit serait donc de permettre à toute personne de garder un contrôle permanent sur ces données.

Le droit à l'oubli numérique compris *latto sensu* semble toutefois peu pertinent. Cela conduit en effet à inclure dans ce droit une multitude de prérogatives, et à en faire une sorte de bric-à-brac aux contours difficilement saisissables.

[39] Ces droits, repris dans les textes européens, sont mentionnées dans la loi « Informatique et Libertés », notamment aux articles 6, 7, 8, et 38 à 43.

Au demeurant, il est important, pour la clarté, l'accessibilité et la cohérence du droit, qu'il existe une adéquation théorique entre la dénomination du droit et son contenu[40]. L' « oubli » numérique vise la seule *disparition* d'une information, et non la maîtrise générale du souvenir à tout instant.

Le droit à l'oubli numérique *stricto sensu*. Il n'existe dans la loi du 6 janvier 1978, ainsi que dans les textes européens et communautaires, que deux dispositions permettant à un individu d'obtenir la disparition de ses données à caractère personnel, sensibles ou non. L'une s'applique *ab initio*, et porte sur la durée de conservation des données, et l'autre s'applique *a posteriori*, permettant d'obtenir l'effacement de ces données.

Ainsi, l'article 6.5° de la Loi du 6 janvier 1978[41], fait obligation au responsable de traitement de ne conserver les données personnelles que « pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ». C'est cette disposition (dite aussi « droit à la péremption des données ») qui serait selon Alain Bensoussan, la véritable expression – bien qu'implicite – d'un droit à l'oubli numérique[42]. La formulation relativement souple de cette obligation a vocation à tenir compte des spécificités de chaque traitement. Elle pose néanmoins des questions d'interprétation – qu'est-ce qu'une durée « nécessaire » ? – qui seront développées par la suite.

La deuxième disposition quant à elle, correspond à un droit dont l'individu peut user, de manière ponctuelle. Il s'agit du droit de demander l'effacement de ses données à caractère personnel (droit à l'effacement). Ce droit est précisé à l'article 40 de la loi Informatique et Libertés[43]. L'article prévoit en effet que « toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient […] effacées les données à caractère personnel la concernant, qui […] périmées, ou dont la

[40] On rappellera à ce titre que le Conseil constitutionnel a estimé que l'accessibilité et l'intelligibilité de la loi est un objectif à valeur constitutionnel : (voir par exemple 421 DC du 16 décembre 1999, ou encore 475 DC du 24 juillet 2003).

[41] Voir également : article 5.e de la Convention n°108 du Conseil de l'Europe ; article 6.1.e de la directive 95/46/CE.

[42] Alain BENSOUSSAN, *L'informatique et le droit*, Ed. Hermes, 694 pp. 1994, p. 466.

[43] Voir également : article 8.c et d de la Convention n°108 du Conseil de l'Europe ; article 6.1.d et 12. b. de la directive 95/46/CE.

collecte, l'utilisation, la communication ou la conservation est interdite ». Ainsi, de manière générale – nous reviendrons plus loin sur les questions d'interprétation de cette disposition – toute personne physique disposerait d'un droit à obtenir l'effacement de ses données personnelles dont la conservation ne serait plus nécessaire au vu des finalités du traitement dont elles feraient l'objet.

En définitive, le droit à l'oubli numérique correspondrait, en l'état actuel du droit, à l'application conjointe de l'obligation qu'a le responsable de traitement de ne pas conserver des données à caractère personnel au-delà de la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées, et du droit de toute personne physique à l'effacement de ces données lorsqu'une telle obligation n'est pas respectée.

2. Vers une consécration explicite du droit à l'oubli numérique ?

A l'heure actuelle, seul un jugement, rendu par le TGI de Paris en référé, a consacré explicitement un « droit à l'oubli[44] ». Les différents textes existants ne le garantissent, eux, que de manière implicite, à l'exception de la Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche[45](a). Il est cependant question de l'inscrire dans le droit positif (b).

a. La Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche

La *Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche*, signée à Paris le 13 octobre 2010 fait suite à une réflexion lancée au niveau national par Madame Nathalie Kosciusko-Morizet, alors Secrétaire d'État chargée de la Prospective et du Développement de l'économie numérique.

Le texte, qui concerne les données personnelles publiées volontairement sur les sites collaboratifs et les moteurs de recherche, poursuit deux objectifs : d'une part,

[44] TGI Paris, Vernes c. SAS les Échos, *op., cit.*

[45] Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche, signée à Paris, le 13 octobre 2010, sous l'impulsion de Madame Nathalie KOSCIUSKO-MORIZET, alors Secrétaire d'Etat chargée de la prospective et du développement de l'économie numérique.

améliorer la transparence de l'exploitation qui est faite des données publiées par les internautes, d'autre part permettre à ces internautes d'exercer un « meilleur contrôle sur ces données ». Les signataires sont alors invités à prendre plusieurs mesures, telle que la mise en œuvre d'action de pédagogies (article 1.1), la protection des données personnelles contre l'indexation automatique par les moteurs de recherche (article 2), l'incitation à fournir, dès la page d'accueil « un lien vers une information conviviale et facilement accessible sur leur politique de protection de la vie privée » (article 1.2), la mise à disposition de l'internaute d'outils permettant de gérer les données qu'il publie (article 3), la mise en place de « dispositifs permettant de vérifier si les utilisateurs sont mineurs » (article 4.1), la mise en place d'un outil de signalement et d'un bureau de réclamations (article 5), et enfin la possibilité de maintenir un haut niveau de protection des données en cas de transfert vers un prestataire tiers (article 6).

Le « droit à l'oubli numérique » n'est cependant pas visé dans le corps de la Charte. Sa mention expresse est à rechercher dans le Préambule. Selon ce dernier, la Charte a vocation à mettre en œuvre les « droits constituant le "droit à l'oubli" ». Le texte poursuit en précisant qu'il s'agit de matérialiser les principes de finalité, de consentement, de droit à l'information, de droit d'accès, de rectification et d'opposition, prévus par la loi Informatique et Libertés ou, le cas échéant par les autres textes ou traités internationaux en vigueur ». La Charte semble donc adopter une approche extrêmement large du droit à l'oubli numérique. Elle ne le restreint pas à la limite de la durée de conservation des données à caractère personnel et au droit de suppression. Au contraire, elle semble l'étendre à chacun des droits prévus par la loi « Informatique et Libertés », soit le droit à l'information, la nécessité de recueillir le consentement de l'intéressé, le droit d'accès, le droit d'opposition, et le droit de rectification de modification et d'effacement.

Certes, la Charte a le mérite de venir concrétiser par un texte – non contraignant – les débats qui ont eu lieu depuis l'atelier organisé à Sciences-Po Paris en 2009, et d'entraîner une prise de conscience de l'opinion publique, par sa médiatisation, des enjeux de la protection des données.

Néanmoins, pour les raisons que nous avons développées plus haut, la conception large du droit à l'oubli numérique qu'elle véhicule ne semble pas permettre à terme, sa consécration en droit positif. L'absence de définition précise de ce droit conjuguée au large écho dont s'en font les médias risquent de rendre sa compréhension difficile au grand

public, et même au juriste. Le droit à l'oubli numérique devient alors un simple outil de communication ou, comme le disent certains, une sorte de *buzzword*, destiné à sensibiliser plutôt qu'à protéger.

Toutefois, la portée de cette Charte est à relativiser. En effet, des acteurs privés tels Google et Facebook, qui sont des acteurs incontournables du web n'ont pas accepté de la signer[46], de même que la CNIL, malgré sa participation aux différentes réunions préalables à l'élaboration du texte.

Une solution plus probante pourrait être la consécration positive du droit à l'oubli numérique.

b. Vers une consécration explicite du droit à l'oubli numérique en droit positif

Cette consécration a déjà été envisagée en droit national, ainsi qu'à l'échelle européenne, plus récemment.

Vers une consécration à l'échelle nationale ? Le terme même de « droit à l'oubli » n'était pas ignoré des rédacteurs de la loi du 6 janvier 1978. Ainsi, le sénateur Jacques Thyraud écrivait déjà, en 1977 : « L'informatique […] a introduit […] une capacité de mémorisation considérable au point que certains peuvent craindre qu'elle ne porte atteinte à l'un des droits les plus fondamentaux de l'être humain : le droit à l'oubli[47] ». En 1978, le choix a cependant été fait de ne mentionner ce droit dans la loi que de manière implicite.

Récemment pourtant, un rapport parlementaire a proposé de le consacrer explicitement. Il fait suite à une réflexion sur le respect de la vie privée à l'heure des mémoires numériques, initiée fin 2008 à la demande de la commission des lois du Sénat

[46] Dans un communiqué, la firme a notamment estimé que « les Internautes doivent pouvoir contrôler eux-mêmes leurs données personnelles sur Internet et parmi nos services, nous proposons déjà de nombreux outils qui offrent transparence et choix aux utilisateurs ». Communiqué disponible en partie à l'adresse : http://www.numerama.com/magazine/17048-google-explique-pourquoi-il-n-a-pas-signe-la-charte-sur-le-droit-a-l-oubli.html.

[47] Rapport n° 72 (1977-1978) de M. Jacques THYRAUD, fait au nom de la commission des lois, déposé le 10 novembre 1977.

par les sénateurs Anne-Marie Escoffier et Yves Détraigne. Leur mandat consistait à conduire une étude sur les « technologies de traçabilité » capables de pister les individus dans l'espace (biométrie, vidéosurveillance, géolocalisation, nanotechnologies, réseaux sociaux …) et dans le temps (moteurs de recherche notamment). A l'issue de leurs recherches, les deux sénateurs ont notamment préconisé la consécration d'un « droit à l'oubli [qui] pourrait s'exercer devant le juge à tout moment[48] ». Selon les auteurs du rapport, il incomberait alors à ce juge de concilier un tel droit avec d'autres droits tel que le droit à la liberté d'expression, et il appartiendrait au demandeur de démontrer « que les faits ou les propos rapportés ne correspondent plus à son mode de vie ou à ses opinions et qu'ils lui causent un préjudice dans sa vie familiale ou professionnelle[49] ». Les sénateurs en conclusion recommandaient de réfléchir à la création d'un droit à « l'hétéronymat » et d'un droit à l'oubli[50]. La proposition de loi qui s'en est suivie n'a cependant pas tenu à consacrer explicitement ces droits[51]. Si elle s'est donné pour objectif de garantir une « plus grande effectivité » au droit à l'oubli numérique, elle a néanmoins choisi de le faire en renforçant les autres droits contenus dans la loi du 6 janvier 1978. Ont ainsi été proposés notamment la consécration d'un droit à une information « spécifique, claire et accessible donnée aux personnes » avant et pendant le traitement, et un « droit à la suppression des données ». Le texte a été adopté au Sénat en première lecture le 23 mars 2010, puis transmis à l'Assemblée nationale le 24 mars. Le processus s'est toutefois interrompu puisqu'à ce jour le texte n'a toujours pas fait l'objet d'un examen en séance publique par les députés.

Vers une consécration à l'échelle européenne ? Une réflexion a été récemment lancée par la Commission européenne dans le cadre de la révision de la directive européenne sur la protection des données à caractère personnel du 24 octobre 1995. En effet, à l'époque, des réalités telles que les réseaux sociaux n'étaient pas encore d'actualité,

---

[48] *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information,* Rapport d'information n° 441 (2008-2009) de M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER, fait au nom de la commission des lois, déposé le 27 mai 2009.

[49] *Ibid*.

[50] *Ibid*, Recommandation n°14.

[51] Proposition de loi n°331 *visant à mieux garantir le droit à la vie privée à l'heure du numérique*, présentée Par M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER, Sénateurs, déposée au Sénat le 6 novembre 2009.

et n'ont pas été pris en compte dans la rédaction des textes. Leur impressionnant développement ces dernières années pose donc la question d'une refonte du canevas législatif de la protection des données, à la lumière de ces nouveaux espaces de communication.

Depuis 2009, la Commission a organisé de nombreux débats, et de nombreuses consultations publiques. Elle a également consulté des organes tels que le G29. Dans une communication du 4 novembre 2010, la Commission a annoncé son intention de modifier la directive dans le courant de l'année 2011[52] (aucune proposition de texte concrète n'a été à ce jour rendue publique). Cette communication propose de renforcer les droits de l'internaute, et d'en consacrer de nouveaux. Parmi ces derniers : le droit à l'oubli numérique. Pour la Commission il s'agit de « clarifier » ce droit en vertu duquel « les personnes peuvent obtenir l'arrêt du traitement des données les concernant et l'effacement de celles-ci lorsqu'elles ne sont plus nécessaires à des fins légitimes. Il s'agit, par exemple, du cas dans lequel la personne revient sur son consentement au traitement des données, ou du cas dans lequel le délai de conservation des données a expiré ».

Cette définition du droit à l'oubli – bien que le terme « numérique » ne figure pas dans l'intitulé du droit – rejoint celle que nous avons exposée plus haut. On y retrouve les deux éléments majeurs de ce droit : le droit à l'effacement des données, et l'obligation de ne traiter les données que pour une durée déterminée. Reste à savoir d'une part, si le texte final reprendra cette analyse, et d'autre part si la nouvelle directive se bornera à « clarifier » le droit à l'oubli numérique, ou bien le consacrera explicitement.

Il est enfin à noter que la communication envisage de consolider les autres droits de l'internaute, depuis la mise en place jusqu'à la fin du traitement, afin de permettre un « oubli » véritable, le cas échéant. Il est ainsi préconisé d'améliorer les modalités d'exercice du droit d'accès, de rectification et de verrouillage, de renforcer le principe de minimisation des données, et surtout, d'assurer un droit à la « portabilité des données ». Ce droit, qui assurerait une quasi-propriété de l'internaute sur ses données, permettrait par exemple de retirer ces dernières d'une application ou d'un service, pour les transférer vers une autre application ou un autre service tiers.

[52] Communication de la Commission au Parlement européen, au Conseil, au Comite économique et social européen et au Comité des régions : «Une approche globale de la protection des données à caractère personnel dans l'Union européenne» ; Bruxelles, le 4.11.2010 COM(2010) 609 final.

En somme, si le droit à l'oubli numérique n'apparaît qu'implicitement consacré en droit positif, il n'est pas exclu que les réformes du droit de la protection des données à l'échelle européenne le consacre expressément. Quoiqu'il en soit, qu'il s'agisse des textes existants ou des textes à venir, tous doivent nécessairement prendre en compte les droits qui pourraient entrer en concurrence avec le droit à l'oubli numérique, voire s'y opposer.

B. Les frontières du droit à l'oubli numérique

Le droit à l'oubli numérique doit être envisagé de manière stricte. Il ne doit donc pas être confondu avec d'autres droits, qui permettent eux aussi la disparition d'une information, même s'il entretient avec eux des liens étroits (1). Le droit à l'oubli numérique peut aussi s'opposer à d'autres droits, et en particulier au droit à la liberté d'expression (2).

1. La frontière entre le droit à l'oubli numérique et les différents droits permettant la disparition d'une information

Le droit à l'oubli numérique entretient des liens étroits avec les différentes dispositions permettant d'obtenir le retrait de certains contenus (a). De même, le droit à l'oubli numérique est proche du droit au respect de la vie privée (b) et de l'ensemble des droits mentionnés dans la loi du 6 janvier 1978 et les textes européens (c)

a. Le droit au retrait de certains contenus

Dans un sens encore plus large, le droit à l'oubli numérique comprendrait, pour certains, tout l'arsenal juridique dont disposerait une personne pour obtenir la suppression d'une donnée[53]. Il renverrait alors non seulement aux droits garantis par les législations

[53] Pour un avis en ce sens, Jean-Christophe DUTON et Virginie BECHT : « Le droit à l'oubli numérique : un vide juridique ? », *Le journal du Net*, 24/02/2010.

européenne et française en matière de protection des données, mais aussi à toute disposition permettant d'obtenir le retrait d'un contenu illicite ou attentatoire à la vie privée. Ces dispositions figurent dans la loi du 21 juin 2004 pour la confiance dans l'économie numérique[54] (ci-après LCEN), ainsi qu'à l'article 27 de la loi dite « Hadopi II[55] », ou encore à l'article 9 du Code civil[56].

Ainsi, au terme de l'article 6.II de la LCEN, un internaute est fondé à obtenir le retrait d'un contenu illicite, ou manifestement illicite. De la même manière, selon l'article 27 de la loi dite « Hadopi II », le directeur ou le codirecteur de publication d'un service de presse en ligne, dès le moment où il en a connaissance, doit agir promptement pour retirer des données litigieuses ou rendre leur accès impossible dans les espaces publics de contributions personnelles qu'ils dirigent, s'il veut s'exonérer de leur responsabilité pénale. Enfin, l'internaute pourrait obtenir du juge le retrait d'un contenu ou d'une information afin d'empêcher ou de faire cesser une atteinte à l'intimité de la vie privée, au titre de l'article 9 du Code civil.

Sans rentrer dans le détail de ces dispositions, qui nécessiteraient une analyse trop approfondie par rapport au cadre de la présente étude, il est possible d'esquisser par quelques exemples, mais aussi par certaines interrogations, ce que serait le cadre du droit au retrait de certains contenus sur les réseaux sociaux.

Les réseaux sociaux, des hébergeurs ? On considère traditionnellement qu'un hébergeur est une personne, physique ou morale, dont l'activité consiste essentiellement à fournir de l'espace sur ses serveurs pour héberger ou stocker tous types de données (sites web, pages personnelles, etc.). Il a donc une responsabilité plus limitée qu'un éditeur de contenu, puisqu'il n'est pas censé exercer un contrôle sur le contenu publié. Ainsi, aux termes de la LCEN, l'existence d'un contenu manifestement illicite doit être portée à la connaissance d'un « hébergeur », qui a ensuite l'obligation « d'agir promptement » (article 6.II de la LCEN). La notion de savoir si les réseaux sociaux sont des hébergeurs est cependant sujette à discussion. Sans prétendre trancher le débat, il convient néanmoins de

[54] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[55] LOI n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

[56] Cet article permet au juge civil de prescrire toutes mesures propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée, y compris en référé.

relever que le TGI de Paris, dans une ordonnance de référé rendue le 13 avril 2010, a reconnu que le réseau social Facebook, en tant qu'hébergeur, avait l'obligation de retirer des contenus litigieux constituant une atteinte au droit à l'image[57].

Le contenu « manifestement illicite » : Le Conseil constitutionnel, dans sa décision du 10 juin 2004 portant sur la LCEN, a émis une réserve en estimant qu'un hébergeur ne pouvait pas être juge du caractère illicite d'un contenu, mais qu'il devait l'être de son caractère « manifestement illicite[58] ». Le problème est alors l'interprétation de ce qu'est un contenu manifestement illicite. Le contenu illicite serait par exemple, en France, un contenu qui constituerait des infractions pénales, telle que la mise en ligne de menaces (art. 222-17 et 222-18 du code pénal), d'injures non publiques (art. R. 621-2 du code pénal), ou plus généralement, d'un contenu qui constituerait une atteinte à la vie privée (articles 225-1 à 226-7).

Les infractions de presse : Le droit au retrait de certains contenus, si l'on estime que les réseaux sociaux sont des hébergeurs, pose également la question de la nature publique ou privée de ces réseaux. En effet si, comme certains l'estiment[59], ils constituent des espaces de communication publics, le spectre du contenu dont il serait possible d'obtenir la suppression serait passablement étendu, en particulier à certaines infractions de presse. On pourrait alors imaginer le retrait d'un contenu diffamatoire, ou contenant des injures publiques (art. 29, alinéa 2, de la loi du 29 juillet 1881 sur la liberté de la presse), ou la saisine du juge des référés, en application de l'article 50-1 de la loi du 29 juillet 1881,

[57] TGI Paris, *ord. réf., H. Giraud c./ Facebook France*, 13 avril 2010. En l'espèce, un évêque se plaignait de la diffusion de son image sur une page Facebook intitulée « Courir nu dans une église en poursuivant l'évêque ainsi que de la mise en ligne de divers commentaires à son sujet. Le juge a estimé que diffusion de l'image du défendeur, en l'absence de toute explication et justification fournies par la défense, et en l'absence de tout consentement, constituait une atteinte au droit à l'image du demandeur prévu par l'article 9 du code civil.

[58] Conseil constitutionnel, 2004-496 DC, 10 juin 2004 : « Considérant que les 2 et 3 du I de l'article 6 de la loi déférée ont pour seule portée d'écarter la responsabilité civile et pénale des hébergeurs dans les deux hypothèses qu'ils envisagent ; que ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge ».

[59] De nombreux auteurs estiment que les réseaux sociaux peuvent être apparentés à des espaces de communication publics (sauf profils fermés au tiers) dès lors que beaucoup d'utilisateurs, professionnels ou non, ont des profils ouverts au public.

pour que soit ordonné l'arrêt du service de communication au public en ligne, dès lors qu'il contient des messages appelant à la commission de crimes ou délits ou provoquant à la haine, à la violence ou à la discrimination et qu'il constitue un trouble à l'ordre public, ou le délit de diffamation. De manière plus générale, on pourrait penser à l'article 6-18 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, aux termes duquel l'autorité judiciaire peut prescrire sur référé ou sur requête toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.

Le droit applicable : En dernier lieu, le retrait de certains contenus suppose de déterminer, en cas de litige opposant l'utilisateur à un réseau social étranger, la détermination du droit applicable, afin de savoir d'une part selon quelle loi apprécier l'illicéité ou non de ces contenus, et d'autre part si la LCEN qui permet d'en obtenir la suppression est applicable.

Quoiqu'il en soit, il semble que le droit au retrait de certains contenus ne corresponde pas véritablement à la définition qui a été proposée du droit à l'oubli numérique. Car si d'un point de vue pratique ces droits ont tous vocation à faire disparaître une information, ils se distinguent d'un point de vue théorique. En effet, le droit au retrait de certains contenus ne s'inscrit pas dans la perspective d'une protection de la personne contre l'intangibilité de l'information à l'ère numérique. Autrement dit, la question du temps de conservation de cette information n'est pas vraiment pertinente dans la mise en œuvre ce droit. Ce qui importe, c'est qu'il existe un contenu illicite, portant atteinte à la vie privée, ou à la réputation d'une personne. En réalité, le droit à la suppression de ces contenus n'est autre que le prolongement sur Internet de certaines infractions ou atteintes à la vie privée déjà existantes. Il s'agit donc plutôt de limiter les abus à la liberté d'expression, que de limiter la conservation des données dans le temps.

Toutefois, il est évident que le droit au retrait de certains contenus peut constituer un outil efficace pour une personne qui souhaite voir disparaître, après un certain temps, une information qu'elle croyait oubliée et qui lui porte préjudice.

b. Le droit à l'oubli numérique et le droit au respect de sa vie privée

Le droit au respect de la vie privée est consacré dans de nombreux textes, tant à l'échelle internationale, qu'à l'échelle européenne, ou qu'à l'échelle nationale. Il est particulièrement présent dans le domaine de la protection des données. Pour certains auteurs, le droit à l'oubli numérique s'inscrit dans le cadre du droit au respect de la vie privée[60]. En effet, en pratique, il est fort probable que le droit à l'oubli numérique ne soit invoqué que dès lors que l'information indûment conservée porte atteinte à la vie privée de la personne.

Il semble toutefois que le droit à l'oubli numérique et le droit au respect de la vie privée, s'ils peuvent concorder (dans le cas par exemple, ou la résurgence du souvenir numérique porte atteinte à la vie privée de la personne), n'existent pas sur les mêmes plans. Le droit à l'oubli numérique s'envisage en effet dans le temps, alors que le droit au respect de la vie privée n'a de sens que si on l'envisage dans l'espace. Ainsi, la vie privée correspond à une sphère d'intimité, c'est-à-dire à un *espace* privé dans lequel on cherche à minimiser toute forme d'ingérence (on cherche à *priver* la plupart des gens de l'accès à cet espace). Cet *espace* n'existe que négativement, par opposition à l'*espace* public. En revanche, le concept d'oubli ne se justifie que dans un rapport au temps. Il ne s'agit pas tant de préserver le droit à la vie privée de la personne, que de protéger cette dernière, à un instant « t+1 » de la résurgence dommageable et de la conservation intemporelle du « souvenir numérique » forgé à un instant « t ».

Le droit à l'oubli numérique en d'autres termes, est centré autour de l'évolution de la personne humaine. C'est ce qu'exprime Alex Türk, président de la CNIL, lorsqu'il écrit qu'il « est inacceptable et dangereux que l'information mise en ligne sur une personne ait vocation à demeurer fixe et intangible, alors que la nature humaine implique, précisément, que les individus changent, se contredisent, bref, évoluent tout naturellement[61] ». Le droit à l'oubli numérique doit donc permettre, dans le temps, de « changer de vie[62] ».

---

[60] Cela semble être par exemple l'approche retenue par la Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche, ainsi que par de nombreux auteurs (voir notamment A. BELLEIL, op.cit.).

[61] Alex Türk, *Commission Nationale de l'Informatique et des Libertés*, 30e rapport d'activités, 2009, p.29.

[62] *Ibid*.

Il convient alors de se demander si les textes qui garantissent un droit à l'oubli numérique permettent de dissocier théoriquement ce dernier du droit au respect de la vie privée, ou au contraire rattachent à ce dernier tous les droits relatifs à la protection des données à caractère personnel.

Or justement, il apparaît que le droit au respect de la vie privée n'est pas le seul objectif poursuivi par les législations européenne et/ou française en matière de protection des données. L'article 1 de la Convention n°108 du Conseil de l'Europe prévoit ainsi que la protection des données concerne le respect pour toute personne physique « de ses droits et libertés fondamentales, et *notamment* (nous soulignons) de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ». Le terme « notamment » indique expressément que la protection des données ne se résume pas à la seule protection de la vie privée. La Directive 95/46/CE elle aussi, affirme dans son article 1.1 son objectif de protection des « libertés et droits fondamentaux », et « notamment » de droit au respect de la vie privée. La Charte des droits fondamentaux quant à elle, fait un pas supplémentaire en distinguant formellement le droit au respect de la vie privée (mentionné à l'article 7), de la protection des données (article 8). Enfin, la loi française de 1978, en son article 1er, se donne pour objectif la protection de « l'identité humaine », des « droits de l'homme », de la « vie privée », et des « libertés individuelles ou publiques » face au développement de l'informatique. Par conséquent, les différents textes de référence en matière de protection des données, s'ils entretiennent des liens étroits avec le concept de vie privée, permettent l'expression et la protection de droits qui poursuivent d'autres objectifs. C'est précisément le cas du droit à l'oubli numérique.

Ainsi, il serait possible de considérer, au sens de l'article 1er de la loi Informatique et Libertés, que le droit à l'oubli numérique de manière générale vise à protéger « l'identité humaine ». On rejoindrait alors les propos d'Alain Bensoussan, qui estimait en 2009 que la vocation du droit à l'oubli numérique est de protéger la « dignité » de la personne, davantage que sa vie privée[63]. Le problème est que la portée et la définition du concept de dignité ne fait aujourd'hui pas l'objet d'un véritable consensus. En outre aucun droit de l'homme, ni aucun des droits fondamentaux ne consacre expressément le droit à l'oubli numérique.

[63] Propos tenus lors de la conférence sur le droit à l'oubli numérique à Sciences-Po Paris, organisée le jeudi 12 novembre 2009 par Nathalie Kosciusko-Morizet, alors secrétaire d'État en charge de la prospective et du développement de d'économie numérique.

En définitive, si le choix de rattacher le droit à l'oubli numérique du droit au respect de la vie privée ne semble donc pas pertinent d'un point de vue conceptuel, il peut être compris en pratique, comme la volonté de le rattacher à un droit fondamental ou à un droit de l'homme, à défaut de consécration expresse. Dans cette perspective, la notion de vie privée serait à envisager dans un sens large[64]. Il faudrait considérer qu'elle s'étend non seulement dans l'espace, mais aussi dans le temps. La résurgence dommageable de l'information indûment conservée constituerait alors une atteinte à la vie privée.

c. Le droit à l'oubli numérique et les droits énoncés dans la loi du 6 janvier 1978

Le droit à l'oubli numérique entretient encore des liens étroits avec les droits garantis par la législation sur la protection des données, et tout particulièrement avec le droit d'opposition.

Les droits garantis par les législations relatives à la protection des données : Les tentatives récentes visant à renforcer le droit à l'oubli numérique illustrent bien la connexité du droit à l'oubli avec les droits contenus dans la loi du 6 janvier 1978 (essentiellement le droit à l'information, le droit d'accès, le droit d'opposition, et le droit à la rectification et à la modification des données). Ainsi, qu'il s'agisse du communiqué annonçant la révision de la Directive 95/46/CE, ou de la proposition de loi française de 2010, tous deux envisagent de permettre une meilleure effectivité du droit à l'oubli numérique à travers le renforcement de ces autres droits. Quant à la Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche de 2010, elle semble aller jusqu'à le considérer comme regroupant tous ces droits.

Tout ceci illustre la difficulté de détacher en pratique le droit à l'oubli numérique des autres droits contenus dans la loi du 6 janvier 1978 et les textes européens. Pour

[64] Une telle interprétation n'est pas inenvisageable. En effet, la Cour européenne des droits de l'homme a considéré que la notion de vie privée devait être comprise comme une notion large (*Peck c. Royaume-Uni,* no. 44647/98, § 57, CEDH 2003-I ; Pretty c. Royaume-Uni, no. 2346/02, § 61, CEDH 2002-III), qui ne pouvait être définie de manière exhaustive (Niemietz c. Allemagne, arrêt du 16 décembre 1992, Série A no. 251-B, p.33, § 29).

prendre un exemple concret, si une information est mise en ligne sur un réseau social, puis diffusée, notamment par l'intermédiaire de moteurs de recherche ou de personnes ayant eu accès au profil de l'intéressé, puis traitée à nouveau par d'autres personnes ou d'autres organismes, il sera impossible de la faire disparaître totalement.

Ainsi, le droit à l'oubli numérique se situant, *ratione temporis*, au bout de la chaîne des droits relatifs à la protection des données, il est impératif de garantir l'effectivité de tous les autres droits, afin de pouvoir accéder à la donnée traitée, connaître l'état et les modalités du traitement, être informé de son éventuel transfert et *in fine*, exercer son droit à l'oubli numérique.

Droit à l'oubli numérique et droit d'opposition : Ce droit est inscrit dans les textes européens et dans la loi du 6 janvier 1978. Selon l'article 38, toute personne a « le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Certains considèrent que le droit à l'oubli numérique comprendrait le droit d'opposition[65]. En effet s'il est invoqué pour des motifs légitimes, le responsable de traitement n'est pas autorisé à procéder à un tel traitement, et n'est donc plus autorisé à conserver lesdites données : il doit les supprimer. Toutefois, le droit d'opposition, ainsi que sa terminologie l'indique, vise l'opposition à un traitement de données, et non la suppression d'une donnée. Dans la chaîne de l'exercice des droits évoquée plus haut, il s'exerce donc en amont du droit à l'oubli numérique, avant le traitement. En pratique cependant, le droit d'opposition s'exerce souvent après la mise en œuvre du traitement, notamment parce que l'intéressé n'en a pas eu connaissance.

Ainsi, il n'est pas exclu, comme le rappelle M. Frayssinet, que le juge conçoive le droit d'opposition de manière extensive, et analyse le droit d'opposition pour motif légitimes en une sorte de droit à la suppression des données[66]. C'est ce qu'a considéré le TGI de Paris en référé, pour qui le droit d'opposition « a vocation à être invoqué en soutien d'une demande de suppression d'un article ancien qui n'aurait fait l'objet d'aucune contestation sur le fondement du droit de la presse mais dont il résulterait des circonstances

[65] Voir par exemple Joël BOYER : « Droit à l'oubli, droit de suppression, droit de suite : la loi Informatique et libertés doit-elle arbitrer la liberté d'expression ? » in *Légicom (Paris), 46. La presse en ligne : Actes du Forum Légipresse du 7 octobre 2010 / Claude Weill / Paris : Victoires éditions – 2011.*

[66] Jean FRAYSSINET : « le pseudo droit à l'oubli appliqué à la presse », *Légipresse*, n°276, Octobre 2010, pp 273-279.

particulières et légitimes au sens de la loi du 6 janvier 1978 que sa libre accessibilité par internet des années plus tard, sans restriction ni limite, serait de nature à causer à la personne concernée un préjudice qui, dans une société démocratique, doit être réparable[67] ».

Si le droit à l'oubli numérique entretient des liens étroits avec les droits évoqués ci-dessus, il semble en revanche s'opposer à la liberté d'expression de tout un chacun.

2. Le droit à l'oubli numérique et la liberté d'expression

A l'instar du droit au respect de la vie privée, la liberté d'expression et d'opinion est protégée au niveau international, européen et national. Elle constitue une limite claire à l'exercice du droit à l'oubli numérique.

Ainsi, la Convention n°108 affirme dans son préambule l'engagement des Etats « en faveur de la liberté d'information sans considération de frontières ». De la même manière, la directive européenne 95/46 (article 9) invite expressément les Etats à adopter des exemptions et dérogations pour les traitements « effectués aux seules fins de journalisme ou d'expression littéraire et artistique ». C'est ce qu'a fait la loi « Informatique et Libertés » à l'article 67.

De manière plus générale, le droit à l'oubli numérique ne peut en aucun cas constituer un outil à la discrétion de l'individu, pour restreindre la liberté d'expression d'autrui. C'est d'ailleurs ce qu'a estimé le TGI de Paris, dans une ordonnance de référé du 12 octobre 2009, en rappelant que « le principe constitutionnellement et conventionnellement garanti de la liberté d'expression interdit de retenir une atteinte distincte liée à une éventuelle violation des règles instituées par la loi du 6 janvier 1978,

[67] TGI Paris, ord. réf., 25 juin 2009, *op., cit.*

laquelle n'est pas une des normes spécialement instituées pour limiter cette liberté dans le respect du second alinéa de l'article 10 de la convention européenne susvisée[68] ».

En définitive, l'analyse théorique du droit à l'oubli numérique permet de définir ce dernier comme le droit de ne voir ses données personnelles traitées que pour une durée nécessaire et limitée d'une part, et le droit à l'effacement de ces données passé un tel délai d'autre part. Il est éventuellement possible selon une conception large, d'y inclure également le droit d'opposition pour motifs légitimes. Le droit à l'oubli numérique ne peut en revanche pas porter sur les données publiées par un autre internaute, qui agit dans le cadre de sa liberté d'expression. Si toutefois ces données revêtaient un caractère illicite, il serait possible d'en obtenir le retrait, sur le fondement non pas du droit à l'oubli numérique, mais d'autres droits, tel que le droit au respect de la vie privée, ou le droit au retrait d'un contenu illicite garanti par la LCEN et la loi « Hadopi II ». Ces droits, ainsi que le droit au respect de la vie privée, s'ils peuvent effectivement aboutir à la suppression d'une information, ont davantage vocation à sanctionner des infractions spécifiques qu'à protéger l'individu contre l'intangibilité de son passé numérique. Ils se distinguent donc du droit à l'oubli numérique.

En pratique ensuite, il est évident que le droit à l'oubli numérique peut difficilement être effectif sans l'exercice préalable des autres droits garantis par les législations européenne et française en matière de protection des données (droit d'accès, droit à l'information, droit d'opposition, etc.).

La question se pose alors de la mise en œuvre de ce droit sur les réseaux sociaux, et plus particulièrement de son applicabilité. Cette mise en œuvre pose un grand nombre de questions juridiques, que ni les textes ni la jurisprudence n'ont réellement tranché aujourd'hui. Il sera alors d'abord proposé de l'envisager de manière extensive. On en verra plus loin les inconvénients.

[68] Tribunal de grande instance de Paris Ordonnance de référé 12 octobre 2009 *Mme X, Société L. & Com / Jean-Hervé C.*

II. Approche extensive de l'applicabilité du droit à l'oubli numérique sur les réseaux sociaux

Le choix d'une analyse extensive vise à montrer de quelle manière on pourrait rechercher une applicabilité optimale du droit à l'oubli numérique, afin de pouvoir mieux comprendre ensuite les difficultés qu'elle suscite. Une telle analyse se fonde notamment sur l'avis du G29 de 2005 relatif aux réseaux sociaux[69], auquel le site officiel de la CNIL a d'ailleurs octroyé une large place[70].

L'applicabilité du droit à l'oubli numérique doit être envisagée en deux temps. Il convient de s'intéresser d'abord à la question de son applicabilité *ratione materiae* (A), puis de son applicabilité *ratione loci* (B).

A. L'applicabilité ratione materiae *du droit à l'oubli numérique*

L'article 5 de la loi « Informatique et Libertés » dispose que « sont soumis à la présente loi les traitements de données à caractère personnel dont le responsable est établi sur le territoire français ou dont le responsable, sans être établi sur le territoire français [...] recourt à des moyens de traitement situés sur le territoire français ».

Pour que le droit à l'oubli numérique soit applicable sur les réseaux sociaux, il faut donc qu'il existe un responsable de traitement (1), qui opère un traitement de données à caractères personnelles (2).

1. L'existence d'un responsable de traitement

La notion de « responsable de traitement » n'était pas précisée dans la version initiale de la loi. Ce n'est qu'à l'occasion de la transposition en droit national de la Directive 95/46/CE, qu'une définition a été proposée. Ainsi, selon l'article 3 de la loi modifiée, le responsable de traitement est, « sauf désignation expresse par les dispositions

[69] G29, Avis 5/2009, *op., cit.*.

[70] CNIL, « Le G29 précise les règles applicables aux réseaux sociaux ». Source : http://www.cnil.fr/la-cnil/nos-defis/innovation-et-expertise/actualite-expertise/article/le-g29-precise-les-regles-applicables-aux-reseaux-sociaux/.

législatives ou réglementaires relatives [au] traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ».

La question de savoir qui peut être considéré comme responsable de traitement sur un réseau social mérite d'être posée, en raison de la multiplicité des acteurs intervenant sur ces espaces de communication. Le G29, dans son avis de 2009 a ainsi identifié trois responsables possibles : le fournisseur du service de réseautage social (SRS), le fournisseur d'application, et dans certains cas l'utilisateur lui-même.

Les fournisseurs de SRS : Les fournisseurs de service qui gèrent le réseau sont des organismes privés qui déterminent les finalités et les moyens du traitement. Les moyens sont, ainsi que le rappelle le G29, « tous les services "basiques" liés à la gestion des utilisateurs » tels que « l'enregistrement et la suppression des comptes[71] ». Quant aux finalités, il peut s'agir par exemple de l'utilisation des données des utilisateurs « à des fins publicitaires ou commerciales – y compris la publicité fournie par des tiers[72] ». Les fournisseurs de SRS peuvent donc bien être considérés comme des responsables de traitement, au sens des législations européenne et française.

Les fournisseurs d'applications : La plupart des réseaux sociaux, en complément des services qu'ils fournissent, proposent aux utilisateurs des applications additionnelles fournies par des concepteurs tiers. Ces applications ont des objets divers. Il peut s'agir de jeux en lignes, de questionnaires, de comparateurs voyages, de services météo, etc[73]. Les fournisseurs d'applications peuvent être amenés à traiter des données à caractère personnel des utilisateurs du réseau se servant de leurs applications. Dans ce cas, selon le G29[74], ils doivent eux aussi être considérés comme responsables de traitement.

[71] G29, Avis 5/2009, *op., cit*.., p. 5.

[72] *Ibid*.

[73] Pour une liste des applications sur le réseau social Facebook, voir par exemple le répertoire des applications disponible sur : http://www.applications-facebook.org/repertoire_application.php.

[74] G29, Avis 5/2009, *op., cit*.., p. 5.

Les utilisateurs du réseau : La question de savoir si un utilisateur du réseau peut être considéré comme responsable de traitement est délicate. Il pourrait être en effet considéré qu'il traite lui-même ses données, son inscription volontaire sur un réseau social aux fins de partager des informations revenant à déterminer les finalités et les moyens du traitement. Par ailleurs l'utilisateur peut facilement accéder aux informations publiées par ces contacts, et les utiliser à sa guise (les conserver, les enregistrer, les diffuser, etc.). Toutefois, la plupart du temps, l'utilisateur ne « traite » ses données ou celles de ses contacts qu'à des fins personnelles. Dans ce cas, il ne peut être considéré comme un responsable de traitement, puisque ni la Directive 95/46/CE ni la loi du 6 janvier 1978 ne sont applicables aux « traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles » (article 2§1 de la loi française), ou « domestique » (article 3.2 de la Directive). On dit alors que l'utilisateur tombe sous le coup de « l'exemption domestique ».

Il est cependant notoire que les réseaux sociaux ne sont plus un espace de communication réservé aux seuls fins de divertissement et de communication entre particuliers. Ainsi que le rappelle Mme Reding, on serait passé du «Web 2.0 pour les loisirs » au « Web 2.0 pour la productivité et les services »[75]. C'est-à-dire que les entreprises ont désormais couramment recours à ces réseaux, que ce soit dans l'optique du recrutement de futurs employés, ou dans le cadre d'une stratégie *marketing* (valorisation de l'image de l'entreprise, promotion de produits, test ou sondages auprès d'un large public, organisation d'évènements, publicité, etc.[76]). Un utilisateur n'est donc plus forcément un particulier inscrit à des fins uniquement personnelles. Dès lors, selon le G29, si le réseau est utilisé « comme une plate-forme de collaboration pour une association ou une entreprise[77] » qui agit à des fins politiques, commerciales, ou sociales, « l'utilisateur assume [...] l'entière responsabilité d'un responsable du traitement des données[78]».

[75]Discours de Mme REDING, Membre de la Commission européenne responsable de la Société de l'Information et des Médias à propos de l'Initiative « Futur de l'Internet » du Conseil Européen de Lisbonne (2 février 2009): « l'Internet du futur: l'Europe doit jouer un rôle majeur ».

[76] Voir par exemple Emmanuel FRAYSSE : *Facebook, Twitter et le web social, les nouvelles opportunités de business: stratégies, marketing, meilleures pratiques* , Agence Kawa, Numilog, 2e éd., 2011, 346 p.

[77] G29, Avis 5/2009, *op., cit*.., p. 6.

[78] *Ibid*.

2. Un traitement de données à caractère personnel

Il a été considéré plus haut qu'un traitement de données à caractère personnel pouvait être entendu, de manière large, comme toute manipulation de telles données.

L'identification d'un tel traitement ne pose pas de difficulté particulière en ce qui concerne les réseaux sociaux. Les fournisseurs de SRS procèdent en effet à l'enregistrement et à la conservation des informations fournies par les utilisateurs lors de l'inscription, ainsi que des informations publiées par ceux-ci dans le cadre de leur activité sur le réseau. Par ailleurs, les fournisseurs du service de réseautage social (SRS) peuvent utiliser et traiter les informations fournies par les membres à des fins de prospection commerciale (publicité ciblée).

Il faut encore que ces informations puissent être considérées comme des données à caractère personnel, c'est-à-dire des données permettant d'identifier directement ou indirectement une personne physique, aux termes de l'article 2§2 de la loi du 6 janvier 1978. On également vu que la notion avait un caractère large et évolutif. Or, lors de son inscription sur le réseau par exemple, un utilisateur doit la plupart du temps indiquer son nom, son courriel, son âge, son sexe, etc. Ces données permettent incontestablement d'identifier une personne physique, et sont des données à caractère personnel.

On trouve également dans le cadre de l'activité des utilisateurs sur le réseau, des données à caractère personnel qui peuvent être qualifiées de « sensibles », au sens des législations européenne et française. L'utilisateur peut par exemple mettre en ligne toute sorte d'opinion politique ou religieuse, toute pensée ou tout sentiment, ou encore renseigner sur ses préférences sexuelles, ou sur sa santé. Il dispose à cet effet d'une panoplie d'outils tel que le « statut de profil », la possibilité de laisser des « commentaires », « d'aimer » un lien ou toute autre information publiée par un utilisateur, ou encore de laisser un message sur le « mur » d'un contact, etc. (grâce à la fonction « Like », ou en français, « J'aime »). Il est donc raisonnable de penser que les fournisseurs de SRS, et le cas échant les fournisseurs d'application, opèrent des traitements de données à caractère personnel, que ce soit à des fins de gestion des comptes, ou à des fins de prospection commerciale.

Reste à savoir si la loi française qui garantit un droit à l'oubli numérique est applicable *ratione loci* à ces réseaux sociaux.

B. L'applicabilité ratione loci *du droit à l'oubli numérique*

La détermination du champ d'application dans l'espace du droit européen et du droit français est un des défis majeurs pour la protection des données personnelles en Europe. Car les réseaux sociaux, s'ils entendent cibler un public européen, peuvent être localisés en divers endroits, en Europe et hors Europe (notamment aux Etats-Unis). Or, l'application du droit européen et la loi du 6 janvier 1978 est déterminé par un critère de rattachement territorial (1). Ainsi, une fois ce critère identifié, se pose la question de l'applicabilité ou non du droit aux réseaux sociaux établis hors Europe (2).

1. Les critères de rattachement du droit de la protection des données

L'article 4 de la Directive 95/46/CE et l'article 5 de la loi du 6 janvier 1978 mettent en place des critères déterminant respectivement l'application du droit européen et du droit français de la protection des données personnelles. Ces dispositions établissent un critère principal (a), et un critère subsidiaire (b).

a. Le critère principal : l'établissement du responsable de traitement dans l'Union européenne

La Directive 95/46/CE prévoit en son article 4 a) que le droit national de chaque Etat membre de l'Union européenne s'applique lorsque « le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre ». Le même article précise que le responsable de traitement « doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable ».

En France, la loi du 6 janvier 1978 (article 5. I. 1°) reprend le critère de la Directive en soumettant au droit français **«** les traitements de données à caractère personnel dont le responsable est établi sur le territoire français ».

Ainsi, deux cas de figure se présentent. Si le responsable de traitement dispose d'un établissement en France qui participe au traitement des données personnelles, la loi du 6 janvier 1978, et partant, le droit à l'oubli numérique, s'appliquent. Si le traitement est réalisé par un établissement situé dans un ou plusieurs autres Etats membre, le ou les droits

de ces Etats s'appliquent concomitamment. Le droit à l'oubli numérique, inscrit aux articles 6 e) et 12 b) ne joue alors que dans la mesure où les dispositions de la directive ont été transposées en droit interne.

b. Le critère subsidiaire : le recours à des moyens de traitement sur le territoire d'un Etat membre de l'Union européenne

La Directive 95/46/CE prévoit en son article 4 c) que le droit national de chaque Etat membre de l'Union européenne s'applique lorsque « le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté ».

Là encore, la loi française (article 5. I. 2°) s'aligne sur la Directive, en étendant son application aux cas où « le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne ». Dès lors, de manière subsidiaire, si le responsable de traitement n'est pas établi en Europe, il sera tout de même soumis au droit de chaque Etat européen sur lequel il recourt à des moyens de traitement, sauf s'il recourt à des moyens utilisés à des seuls fins de transit.

En ce qui concerne la loi française en particulier, elle est donc applicable si le responsable de traitement dispose d'un établissement en France qui participe au traitement des données personnelles, ou de manière subsidiaire, si le responsable de traitement n'est pas établi en Europe mais recourt à des moyens de traitement en France.

A contrario, l'analyse de ces critères de rattachement indique qu'un responsable de traitement établi hors de l'Union européenne et n'ayant pas recourt à des moyens de traitement, ou si ces derniers ne sont utilisés qu'à des seules fins de transit, ne devrait pas être soumis aux législations européennes et/ou française relatives à la protection des données.

L'applicabilité de ces législations ne pose donc pas, *ratione* loci, de difficulté dans le cas des réseaux sociaux possédant un établissement participant au traitement des données à caractère personnel sur le territoire d'un Etat membre de l'Union européenne. En vertu du critère de rattachement principal développé ci-avant, ils sont soumis à la loi nationale correspondante, qui est censée avoir transposé la Directive 95/46/CE. Toute personne inscrite sur un réseau social possédant un établissement participant au traitement de données personnelles sur le sol européen devrait donc en théorie bénéficier d'un droit à l'oubli numérique. La question est en revanche plus délicate pour les réseaux sociaux établis hors de l'Union européenne.

2. Une applicabilité hétérogène entre les réseaux sociaux établis dans l'Union européenne et hors Union européenne ?

L'applicabilité des législations européenne et/ou française relatives à la protection des données est contestée par les réseaux sociaux n'étant pas établis dans l'Union européenne, et ne reconnaissant pas les sociétés établies sur le sol français comme leurs représentantes ou leurs mandataires[79]. On prendra ici l'exemple des réseaux sociaux américains. La contestation se fonde sur deux arguments : d'abord, les Conditions générales d'utilisation de ces réseaux sociaux écartent la compétence du juge français, ainsi que l'application des législations européennes en cas de litige[80](a), et en tout état de cause, ces réseaux estiment ne pas utiliser de moyens de traitement sur le sol européen (b).

[79] Par exemple, la société mère Facebook Inc. basée aux Etats-Unis, ne reconnaît pas sa filiale Facebook France comme une société la représentant, ou étant mandatée par elle. Elle agirait plutôt comme une société de fourniture de services et de conseils. Ainsi Facebook Inc. ne s'estime pas installée sur le sol français.

[80] Les Conditions générales d'utilisation (ci-après CGU), en anglais "Terms of use" ou "Terms of service" ou encore "terms and conditions", se présentent généralement sous la forme d'une liste de paragraphes ou d'articles qui indiquent les modalités d'utilisation du réseau par l'utilisateur, informent celui-ci de ses droits, et du mode de fonctionnement du réseau social. Les CGU abordent notamment les questions de responsabilité, ainsi que le droit pour le fournisseur de SRS de modifier unilatéralement ses conditions, de mise à jour du réseau, et de droit applicable. Afin de garantir l'opposabilité des CGU aux utilisateurs, les fournisseurs de SRS imposent que ces derniers les « acceptent » lors de leur inscription.

a. L'éviction de la loi française dans les Conditions générales d'utilisation : l'exemple des réseaux sociaux américains

Les CGU de la plupart des réseaux sociaux américains disposent expressément que le droit applicable n'est pas le droit européen, ni la loi française, mais le droit d'un Etat extérieur à l'Union. D'autre part, elles stipulent que seul un juge américain est compétent en cas de litige.

Ainsi – la liste n'est pas exhaustive – Facebook prévoit que toute plainte et toute action entre l'utilisateur et le réseau seront portées « exclusivement devant les tribunaux d'État et fédéraux sis dans le comté de Santa Clara, en Californie […] sans égard aux principes de conflits de lois[81] ». De la même manière, le réseau professionnel LinkedIn prévoit que « les réclamations, les actions en justice ou les différends […] sont régis par les lois de l'État de Californie, quel que soit votre pays d'origine ou le pays depuis lequel vous accédez à LinkedIn et nonobstant les principes des conflits de lois et la Convention des Nations unies sur la vente internationale de marchandises[82] ». On pourrait encore ajouter à cette liste le réseau Google+, qui soumet lui aussi tout différend aux lois et à la « juridiction exclusive des cours du comté de Santa Clara en Californie[83] ». Quant au réseau MySpace, il soumet les différends qui l'opposeraient à ces utilisateurs aux « lois de l'État de New York, sans tenir compte des règles de conflit des lois[84] ».

Il est frappant de constater que ces clauses sont rédigées de manière extrêmement large. Elles ne visent pas seulement le droit applicable (le droit américain), mais aussi le juge compétent (le juge américain). Ainsi, elles seraient tout à la fois des clauses de détermination du droit applicable, et des clauses attributives de juridiction.

En principe, le droit international privé reconnaît la validité de ces clauses. Selon le principe de la loi d'autonomie, les parties peuvent en effet, dans un contrat international, déterminer elles-mêmes quelle juridiction sera compétente et quel sera le droit

---

[81] Facebook, Conditions générales d'utilisation, point 15 (dernière consultation le 23/08/2011). Accessible à l'adresse : https://www.facebook.com/terms.php.

[82] LinkedIn, Conditions générales d'utilisation, point 8.A (dernière consultation le 23/08/2011). Accessible à l'adresse : http://fr.linkedin.com/static?key=user_agreement&trk=hb_ft_userag.

[83] Google+, Conditions générales d'utilisation, point 20.7 (dernière consultation le 23/08/2011). Accessible à l'adresse : http://www.google.com/accounts/TOS?hl=fr.

[84] MySpace, Conditions générales d'utilisation, point 16 (dernière consultation le 23/08/2011). Accessible à l'adresse : http://fr.myspace.com/Help/Terms.

applicable[85,86]. Le problème en l'espèce, c'est que ces clauses semblent aller bien au-delà d'une simple relation contractuelle. En effet, la terminologie utilisée ne concerne pas seulement les litiges afférents aux CGU, mais vise aussi « toute action » intentée contre un réseau social. En d'autres termes, la clause a tout simplement pour effet d'évincer l'application du droit européen et/ou français. Concrètement, cela signifierait que le juge français par exemple, saisi d'un litige concernant un utilisateur français pour non-respect par un réseau social de son droit à l'oubli numérique, au sens de la loi du 6 janvier 1978, ne devrait même pas examiner si oui ou non le réseau social recourt à des moyens de traitement sur le territoire français. Il devrait se dessaisir au profit du juge californien.

Ainsi, accepter l'opposabilité de ces clauses reviendrait *de facto* à accepter que tout réseau social non établi sur le sol de l'Union européenne, par le biais d'un tel montage juridique, puisse se soustraire à l'application de la législation européenne, qu'il recoure ou non à des moyens de traitement dans l'Union. Toutefois, en droit, la possibilité de refuser l'opposabilité de ces clauses renvoie à des problématiques de droit international privé particulièrement complexes, dont le développement nécessiterait une analyse approfondie, qui ne saurait rentrer dans le cadre de la présente étude. On se bornera donc à amorcer une réflexion sur le sujet en soulignant quelques éléments et quelques interrogations, sans prétendre apporter une réponse tranchée à la question.

Le problème de la validité des clauses attributive de juridiction et de détermination du droit applicable : En règle générale, il semble que le juge – du moins en France – doive apprécier la validité d'une telle clause au regard du droit désigné par elle ou par le contrat[87]. Ainsi, dans le cadre des réseaux sociaux désignant les juridictions californiennes comme compétentes, et le droit californien comme droit applicable, le juge devrait apprécier la validité de la clause au regard du droit californien. Si celle-ci s'avérait valable selon ce dernier, il devrait donc en toute rigueur se dessaisir au profit du juge californien.

---

[85] *Messageries maritimes*, Cass., 21 juin 1950, Grands arrêts de la jurisprudence française de droit international privé (5ème éd., 2006), arrêt n° 22, p. 194.

[86] Article 3.1 Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I) *Journal officiel n° L 177* du 04/07/2008 p. 0006 – 0016.

[87] Cass. 1re civ., 3 déc. 1991, *RCDIP* 1992, 340 note H. GAUDEMET-TALLON.

La doctrine et la jurisprudence ne sont toutefois pas unanimes sur la question. Par conséquent, il existe dans de nombreux domaines des règles matérielles permettant, sans s'interroger sur la loi applicable, de déterminer si une clause attributive de juridiction est valable ou non. On pourrait ainsi se demander s'il n'existe pas une règle matérielle qui empêche le choix d'une loi ou d'un juge défavorable à l'utilisateur, considéré comme une partie faible. Il s'agit, autrement dit, de rechercher l'existence d'un ordre public de protection favorable à l'utilisateur. Or, de nombreuses dispositions, dans le droit français et dans le droit communautaire, tant en ce qui concerne la détermination du droit applicable qu'en ce qui concerne la détermination du juge compétent, rappellent un principe de protection du consommateur, face au professionnel. Ainsi, à l'échelle communautaire, le consommateur est protégé par le Règlement Rome I[88], par la Directive 93/13/CEE qui concerne les clauses abusives dans les contrats conclus avec les consommateurs[89], ou encore par le Règlement n°44/2001 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale[90]. Le droit français va lui-aussi dans ce sens en prévoyant que les dispositions relatives aux clauses abusives sont « d'ordre public[91] », et qu'elles s'appliquent « nonobstant toute stipulation contraire[92] ».

A supposer qu'un utilisateur d'un réseau social puisse être considéré comme un « consommateur », il n'est donc pas inenvisageable que le juge considère que les clauses de détermination du droit applicable et attributives de juridictions dans les CGU des réseaux sociaux américains lui soient inopposables, en ce qu'elles défavoriseraient significativement les utilisateurs européens et/ou seraient contraires à l'ordre public. En effet, les législations américaines et en particulier la loi californienne sont beaucoup plus

---

[88] Règlement Rome I, *op., cit.* Le texte dispose ainsi, dans le considérant 23 du préambule, que « s'agissant des contrats conclus avec des parties considérées comme plus faibles, celles-ci devraient être protégées par des règles de conflit de lois plus favorables à leurs intérêts que ne le sont les règles générales ». Voir également l'article 6 du Règlement.

[89] Directive 93/13/CEE du Conseil, du 5 avril 1993, *concernant les clauses abusives dans les contrats conclus avec les consommateurs.*

[90] Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 *concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale* Journal officiel n° L 012 du 16/01/2001 p. 0001 - 0023. Le considérant 14 prévoit ainsi que pour les contrats de consommation il n'est prévu « qu'une autonomie limitée quant à la détermination de la juridiction compétente ».

[91] Article L132-1 du Code de la consommation, al. 9.

[92] Article L135-1 du Code de la consommation : Nonobstant toute stipulation contraire, les dispositions de l'article L. 132-1 sont applicables lorsque la loi qui régit le contrat est celle d'un Etat n'appartenant pas à l'Union européenne, que le consommateur ou le non-professionnel a son domicile sur le territoire de l'un des Etats membres de l'Union européenne et que le contrat y est proposé, conclu ou exécuté.

souples que les législations européennes en matière de protection des données[93]. Ainsi, priver un utilisateur européen de la protection des législations européennes reviendrait à le priver d'une protection « adéquate », au sens de l'article 68 de la Loi Informatique et Libertés[94].

Le problème de l'acceptation des Conditions générales d'utilisation : Le juge pourrait également prendre en considération le fait que souvent, les CGU sont peu lisibles. De fait, peu d'utilisateurs les lisent, notamment les jeunes internautes, et « acceptent » ces Conditions sans même en connaître la teneur. Par ailleurs, « l'acceptation » de ces Conditions n'est souvent qu'indirecte : il est indiqué à l'utilisateur que le fait de cliquer sur le bouton « s'inscrire » signifie qu'il a accepté les CGU, lesquelles ne sont accessibles que par un lien qui renvoie vers une autre page. Concrètement, il peut s'agir du libellé suivant : « En cliquant sur S'inscrire gratuitement, tu acceptes les conditions générales d'utilisation et la politique de confidentialité de [*nom du réseau*] ». Il n'est donc pas certain que le consentement de l'utilisateur soit réellement éclairé. D'autant que beaucoup de mineurs et d'enfants de moins de treize ans fréquentent les réseaux sociaux, malgré l'âge minimum requis à l'inscription, et qui n'ont pas forcément conscience de nouer une relation contractuelle lors de leur inscription[95].

Mais là encore, se pose le problème de la loi à appliquer en ce qui concerne l'appréciation du consentement. Doit-on appliquer la loi californienne ? Peut-on appliquer la loi française, pour des raisons d'ordre public ? Le juge français ne devrait-il pas se dessaisir au profit du juge californien ? Doit-on dissocier l'appréciation du consentement à la clause attributive de juridiction, de celle du consentement aux CGU en général ?

Sans rentrer dans le détail de ces considérations on soulignera que les juges américains eux-mêmes n'ont pas été insensibles au problème de la lisibilité des CGU. Ainsi, même si il ne s'agissait pas d'une affaire relative à des réseaux sociaux, un juge a

[93] Voir pour une analyse de la différence entre ces législations voir l'article de Richard MONTREYRE « Affaire Bénédicte S., Variations sur la détermination de la loi applicable à Google », *Revue Expertises, août septembre 2008, pp.296-300.*

[94] De l'avis de la Cnil et de l'Union européenne, les législations européennes n'offrent pas toujours le niveau de protection requis. Voir par exemple : http://www.cnil.fr/pied-de-page/liens/les-autorites-de-controle-dans-le-monde/.

[95] Voir l'étude réalisée par TNS Soffres pour le compte de la CNIL, *op.,cit*.

estimé, à propos de sites de ventes de tickets en ligne, que la difficulté d'accès des « terms and conditions » empêchait l'établissement d'une relation contractuelle[96]. Dans le même sens, mais cette fois à propos de certaines clauses en particulier, un juge californien, dans l'affaire Mendoza v. AOL, a estimé que des clauses désignant en tant que loi applicable la loi de l'État de Virginie et désignant les tribunaux de cet Etat comme compétents étaient des « clauses cachées», noyées dans un texte peu lisible et peu accessible, et ne pouvaient donc pas être opposées à l'internaute[97].

Par conséquent, il est possible d'imaginer que les clauses de détermination du droit applicable et attributives de juridiction soient contestées, en droit, par le juge français, ou tout autre juge d'un Etat membre de l'Union européenne. Il semble donc raisonnable de penser que le critère décisif pour l'application du droit de la protection des données et du droit à l'oubli numérique aux réseaux sociaux établis hors de l'Union européenne soit l'existence ou non du recours par ces réseaux à des moyens de traitement dans un ou plusieurs Etats membres de l'Union.

b. La question du recours à des moyens de traitement sur le sol européen par les réseaux sociaux établis hors Unions européenne

Les législations européenne et française définissent le traitement comme « toute opération ou tout ensemble d'opérations » portant sur des données à caractère personnel, « quel que soit le procédé utilisé ». Ainsi un moyen de traitement, correspond à un moyen de réaliser toute opération ou tout ensemble d'opération portant sur des données à caractère personnel. Mais ni la Directive 95/46/CE, ni la loi du 6 janvier 1978 ne définissent ce qu'il convient d'entendre par « moyens ». Pourtant, l'interprétation de ce terme a une portée considérable. Elle détermine *in fine* l'applicabilité ou non de la loi à la totalité des réseaux sociaux.

Peu de décisions ont été rendues à ce sujet. En France, la question semble n'avoir fait l'objet que de deux jugements, tous deux rendus par des juridictions statuant en référé

[96] US Federal District Court of Los Angeles *Ticketmaster v. Tickets.com*, 2000 WL 525390 (C.D.Cal.,2000), 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. 2000). Citation originale :« It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with anyone using the website».

[97] Superior Court Of California, *Mendoza v. AOL*, (2000)., County of Alameda, dept. No. 22.

à propos de litiges impliquant non pas des réseaux sociaux, mais le moteur de recherche *Google*. Les deux solutions retenues ne sont d'ailleurs pas motivées de la même manière, et retiennent des solutions contradictoires. Ainsi, le TGI de Paris, le 14 avril 2008 (*Affaire Bénédicte S.*), a écarté l'application de la loi Informatique et Libertés du 6 janvier 1978. Le juge a estimé que la société Google France ne pouvait être considérée comme un « responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation » au sens de l'article 5 de la loi Informatique et Libertés, la société Google France n'exploitant pas le service litigieux et n'étant pas la représentante ni la mandataire de Google lnc. (basée aux Etats-Unis). Par ailleurs, il a considéré, à propos de la société Google Inc. que, en ne disposant d'aucun serveur ni n'utilisant aucun moyen « matériels ou humains » sur le territoire français, celle-ci ne recourait pas à des moyens de traitement de données à caractère personnel sur ce territoire[98]. A l'inverse, le Tribunal de grande instance de Montpellier, par une ordonnance du 28 octobre 2010, (*Marie C. / Google France et Inc*.), a ordonné la désindexation d'une vidéo pornographique mise à la disposition des internautes sans l'accord de l'intéressée, en estimant de manière laconique que la loi Informatique et Libertés était « applicable au moteur de recherche *Google* », au motif que la vidéo faisait l'objet d'un traitement de données à caractère personnel[99].

Ces deux jugements, rendus en référé, donc dans des conditions de délais strictes, ne sauraient fournir une jurisprudence claire en la matière. L'ordonnance de 2008 constatant l'absence de moyens de traitement a par ailleurs été vivement critiquée[100], les auteurs estimant qu'en adoptant une conception stricte de la notion de moyens de traitement (des moyens « matériels ou humains ») elle consacrait l'impunité de la société *Google Inc*.

Ainsi, en l'absence de précisions claires en droit positif, ou de la part de la jurisprudence, les CNIL européennes ont décidé d'adopter une conception extensive de la notion de moyens de traitement. La CNIL française rappelle à ce sujet que l'expression

---

[98] Tribunal de grande instance de Paris Ordonnance de référé 14 avril 2008 *Bénédicte S / Google Inc., Google France*. Source : www.legalis.net.

[99] TGI Montpellier (ord. réf.), 28 octobre 2010, *Marie C. / Google France et Inc. Source* : www.legalis.net.

[100] Richard MONTREYRE « Affaire Bénédicte S., Variations sur la détermination de la loi applicable à Google », *Revue Expertises,* août-septembre 2008, pp.296-300. Voir également A. CAPRIOLI : « Lieu d'archivage des données et loi applicable – Impunité de Google en matière de vie privée sur le territoire français ». *Revue Communication – Commerce électronique*, octobre 2008, p. 44.

« doit s'entendre de manière large[101] ». Par exemple, on peut considérer comme des moyens de traitement « les logiciels de collecte, les formulaires, les serveurs informatiques, les cookies, les bannières Javascript, etc. ». Le G29 a lui aussi adopté une telle approche. Dans son avis de 2009 sur les réseaux sociaux en ligne[102], qui renvoyait à son analyse développée en 2008 à propos des moteurs de recherche[103], il a estimé que constituent des moyens de traitement les « centres de données situés sur le territoire d'un État membre [pouvant] servir au stockage et au traitement à distance de données à caractère personnel », mais aussi « l'utilisation d'ordinateurs personnels, de terminaux et de serveurs », ou encore « l'utilisation de «cookies» et de logiciels similaires par un prestataire de services en ligne ».

Par conséquent, l'ordinateur personnel d'un membre d'un réseau social serait susceptible d'être considéré comme un moyen de traitement, ainsi que toute utilisation par ce réseau de *cookies*. Par conséquent, cette définition permet de considérer – sauf par exemple si le réseau n'utilise pas de *cookies*, ce qui est peu probable – que les réseaux sociaux établis hors de l'Union européenne recourent toujours à des moyens de traitement dès lors qu'ils visent une population située sur le sol européen. Il leur devient alors difficile d'échapper à l'application des différentes lois des Etats dans lesquels ils proposent leur service.

Une autre solution, qui permettrait d'éviter le recours au critère de rattachement territorial et aux difficultés qu'il pose, serait de reconnaître la loi du 6 janvier 1978 en tant que loi de police – ou du moins les dispositions relatives au droit à l'oubli numérique. Il faudrait alors considérer l'application de la loi française comme s'imposant sans contestation possible pour la sauvegarde de l'organisation socioéconomique de la France. Reste qu'aucun juge n'a statué en ce sens. Le TGI de Paris en référé a même écarté expressément cette qualification[104].

---

[101] Voir le site officiel de la CNIL, et plus particulièrement le lien suivant : http://www.cnil.fr/la-cnil/actu-cnil/article/article/a-lheure-de-la-mondialisation-des-echanges-et-des-technologies-sans-frontieres-quelle-loi-app/.

[102] *Op., cit.*. p. 5.

[103] G29, WP 148, *Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche*, pp. 11-13.

[104] Tribunal de grande instance de Paris Ordonnance de référé 14 avril 2008 *Bénédicte S / Google Inc., Google France*. Source : www.legalis.net.

En définitive, bien que les textes de référence en matière de protection des données en Europe et en France n'ont pas intégré les problématiques contemporaines liées aux nouvelles technologies, et en particulier celles liées aux réseaux sociaux, il est possible d'interpréter le droit existant à la faveur d'une large applicabilité du droit à l'oubli numérique sur ces réseaux, qu'ils soient ou non établis dans l'Union européenne. L'analyse repose en particulier sur l'avis du G29 de 2005 relatif aux réseaux sociaux. Il est vrai qu'il s'agit d'un organe consultatif, mais l'impact de ses recommandations ne doit pas être négligé. Les CNIL européennes participent en effet activement aux travaux de l'organe et, en l'absence de texte spécifique aux réseaux sociaux, elles font de l'avis de 2005 une doctrine qu'elles appliquent quotidiennement dans leurs avis, leurs conseils, leurs délibérations, voire dans d'éventuelles mises en demeure ou sanctions.

Il n'en reste pas moins que l'interprétation extensive de la notion de « moyens de traitement » est loin de faire l'objet d'un consensus, et n'a pour l'instant pas été confirmée par la jurisprudence. Une telle approche semble donc davantage fondée en opportunité qu'en droit. Elle répondrait à une volonté affirmée des autorités de protection des données de garantir à toute personne résident dans l'Union européenne la protection du droit européen et, partant, l'exercice d'un droit à l'oubli numérique.

En réalité, le problème de l'applicabilité *ratione loci* du droit à l'oubli numérique n'est qu'un problème parmi d'autres que rencontre la mise en œuvre de ce droit. Car en l'état, l'effectivité du droit à l'oubli numérique sur les réseaux sociaux apparaît assez limitée.

DEUXIEME PARTIE : L'EFFECTIVITE DU DROIT A L'OUBLI NUMERIQUE SUR LES RESEAUX SOCIAUX

La révolution numérique et l'avènement de l'Internet exposent l'homme à la potentielle immuabilité de son passé numérique. Face à cela, les législations relatives à la protection des données en France et en Europe ont permis la reconnaissance d'un droit à l'oubli numérique. Mais l'Internet et la structure des réseaux sociaux remettent en cause la force de ce droit : son effectivité pose de sérieux problèmes en pratique (I). Ces difficultés sont telles qu'elles obligent aujourd'hui à repenser le droit à l'oubli numérique (II).

I. L'effectivité limitée du droit à l'oubli numérique sur les réseaux sociaux

La question de l'existence d'un droit à l'oubli numérique sur les réseaux sociaux a été – elle l'est toujours – largement contestée, pour des raisons d'ordre juridique, mais aussi technique, ce qui rend la mise en œuvre de ce droit complexe, et contestable (A). Cette mise en œuvre est par ailleurs loin d'être homogène, lorsque elle est comparée d'un lieu à un autre, ou d'un réseau à un autre. Autrement dit, le droit à l'oubli numérique fait l'objet d'une mise en œuvre contrastée (B).

A. Une mise en œuvre contestée

Les législations européenne et française qui garantissent implicitement un droit à l'oubli numérique sont antérieures au développement récent et fulgurant des réseaux sociaux, et n'ont donc pas pu prendre en compte les spécificités de ces nouveaux espaces de communications. Par conséquent, la terminologie de ces textes apparaît inadaptée à plusieurs égards : elle est imprécise (1) et parfois peu pertinente (2).

1. La terminologie imprécise des législations françaises et/ou européennes

Le droit à l'oubli numérique pour être effectif, suppose que soient respectées les dispositions qui permettent sa mise en œuvre *a priori*, avec le droit à la péremption des

données (a), et *a posteriori*, avec le droit à l'effacement des données (b). Or les critères d'application de ces deux droits sont largement sujets à interprétation.

a. Le droit à la péremption des données : le problème de la notion de « durée nécessaire ».

Les législations européennes et françaises, dans l'hypothèse où elles sont applicables, imposent une conservation des données à caractère personnel « sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ». Il est cependant difficile sur un réseau social d'identifier à quel moment le traitement d'une donnée à caractère personnel cesse d'être nécessaire.

Selon le G29[105], les données à caractère personnel associées au compte de l'utilisateur doivent être effacées lors de la suppression par celui-ci de son compte.

Quant aux données publiées dans le cadre de l'activité sur le réseau, elles doivent être effacées lors de la mise à jour du compte, lorsque l'utilisateur décide de les supprimer.

Toutefois le G29 admet, pour éviter toute opération malveillante ou toute usurpation d'identité ou pour des raisons sécuritaires, une conservation des informations pour une certaine durée. Or, de telles raisons sont susceptibles d'être invoquées par les réseaux sociaux et de justifier la conservation de données après la suppression du compte par l'utilisateur, ou après la suppression de ses publications.

Ainsi par exemple, la loi pour la confiance dans l'économie numérique (LCEN), complétée par un décret du 25 février 2011, fixe une obligation de conservation des données pendant an, à la charge des hébergeurs et des fournisseurs d'accès à Internet (FAI) [106]. Ces textes ont pour objectif de permettre l'accession à certaines données dans le cadre d'une réquisition judiciaire ou d'une demande administrative prévue par la loi. D'après ces textes, les fournisseurs de SRS ont donc pour obligation, dès lors qu'ils sont considérés

[105] G29, *Avis 5/2009, op., cit.*, p. 11.

[106] Décret n° 2011-219 du 25 février 2011 *relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*, JORF n°0050 du 1 mars 2011.

comme des hébergeurs[107], de conserver pendant un an les identifiants de connexion, l'identifiant attribué par le système d'information au contenu, l'objet de l'opération, les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus, la nature de l'opération (création, modification ou suppression), les date et heure de l'opération et l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni (si par exemple, la personne utilise un pseudonyme pour se connecter ou une adresse de courrier électronique, qu'il y ait une authentification ou une simple déclaration). Les fournisseurs de SRS ont encore l'obligation au sens de l'article 1.3° du décret, de conserver pendant l'année suivant la création du compte, l'identifiant de la connexion, les nom et prénom ou la raison sociale, les adresses postales associées, les pseudonymes utilisés, les adresses de courrier électronique ou de compte associées, les numéros de téléphone, et éventuellement le mot de passe[108]. Ainsi, sans rentrer dans le détail de ces dispositions, les fournisseurs de SRS sont tenus légalement de conserver pendant un an des informations associées aux comptes des utilisateurs.

D'autre part, les fournisseurs de SRS peuvent conserver des informations à des fins de preuve, en prévision d'éventuels litiges qui pourraient les concerner à l'avenir. Dans ce cas, ils peuvent vouloir conserver certaines informations jusqu'à l'extinction des délais de prescription des actions civiles ou pénales, délais qui varient selon les législations nationales. Bien qu'il n'existe pas à notre connaissance de décision judiciaire, ni de texte précisant ce point, il est envisageable que le fait de conserver des données à caractère personnel le temps de l'extinction des délais de prescription soit considéré comme une durée nécessaire au regard des finalités pour lesquelles elles sont traitées.

En définitive, l'appréciation de la durée nécessaire est rendue particulièrement complexe sur les réseaux sociaux par la superposition de plusieurs plans : la durée de conservation des données associées au compte de l'utilisateur et la durée de conservation des données associées à l'activité de l'utilisateur sur le réseau, la conservation à des fins de preuve jusqu'à l'extinction des délais de prescription, et la conservation à des fins légales. Cette complexité rend le droit à la péremption des données difficilement identifiable sur les

[107] Voir les arguments développés en première partie pour reconnaissance des réseaux sociaux en tant qu'hébergeurs.

[108] Il s'agit des cas où il y a un contrat, ou la création d'un compte auprès du fournisseur d'accès ou de l'hébergeur, et dans la mesure où ces données sont collectées. C'est le cas sur un réseau social, puisque l'utilisateur créé un compte auprès du fournisseur de SRS, considéré comme un hébergeur.

réseaux sociaux. Elle le rend également difficilement applicable par les fournisseurs de SRS. Il leur est finalement plus simple de conserver toutes les données pour une durée relativement longue, que de déterminer leur conservation au cas par cas, selon que l'information est associée au compte ou aux publications de l'utilisateur, ou selon la date de suppression du compte de l'utilisateur.

On retrouve les mêmes difficultés d'interprétation dans la mise en œuvre *a posteriori* du droit à l'oubli numérique.

b. Le droit à l'effacement des données et la notion de donnée « périmée »

La notion de péremption est pour le moins floue. D'une manière large, on pourrait considérer que toute donnée supprimée, ou tout compte supprimé, seraient réputés « périmés ». Mais cela reviendrait à donner un champ d'application extrêmement étendu au droit à l'effacement des données et, partant, au droit à l'oubli numérique. En effet, sur un réseau social, cela signifierait que lorsque l'utilisateur supprime une donnée, celle-ci devrait être effacée immédiatement et définitivement par le fournisseur de SRS.

En pratique cependant, une telle conception se heurte à la conservation « nécessaire » des informations par les fournisseurs de SRS après la suppression par l'utilisateur de son compte ou de ses données, pour des raisons de sécurité par exemple. On aurait donc un droit à l'effacement dont le champ d'application théorique serait très large, mais l'effectivité pratique fortement limitée.

La notion de péremption devrait alors être envisagée plus strictement. Elle concorderait soit avec la fin du « délai nécessaire » (on revient alors sur le problème d'interprétation de la notion), soit avec un phénomène de péremption réel, tel un changement d'adresse, un changement de numéro de carte bleue, ou de téléphone.

En somme, il apparaît que l'interprétation des termes des textes rend compliquée la mise en œuvre du droit à l'oubli numérique sur les réseaux sociaux. D'autres notions peuvent elles aussi susciter de nombreuses interrogations, cette fois non pas pour des questions d'interprétation, mais plutôt pour des questions de pertinence.

2. La terminologie peu pertinente des législations françaises et/ou européennes

La question de la pertinence des conditions déterminant *ratione materiae* l'application du droit à l'oubli numérique sur les réseaux sociaux se pose principalement à propos de deux notions : la notion de donnée à caractère personnel (a), et surtout la traditionnelle dichotomie responsable de traitement/sous-traitant (b).

a. La notion de donnée à caractère personnel sur les réseaux sociaux, une appréciation au cas par cas

Pour que le droit à l'oubli numérique soit appliqué, sur les réseaux sociaux, il faut qu'il existe des données à caractère personnel concernant une personne, ces données constituant ce qu'il a été proposé d'appeler le « souvenir numérique ». La notion de donnée à caractère personnel est cependant controversée, comme en témoignent les débats relatifs à l'adresse IP[109].

Or, un réseau social est susceptible de concentrer un nombre extrêmement important de données permettant d'identifier directement ou indirectement une personne physique. Par exemple, une image sur un réseau social peut être « taguée ». C'est-à-dire qu'un utilisateur peut identifier nommément les personnes qui figurent sur une image qu'il met en ligne[110]. Dès lors, bien qu'on ait pu discuter du fait qu'il s'agisse ou non d'une donnée à caractère personnel[111], il ne fait guère de doute qu'une image « taguée » permet d'identifier directement une personne, et constitue une donnée à caractère personnel. La potentialité d'identification directe à partir d'une image a d'ailleurs été renforcée avec le

[109] La CNIL (Communiqué du 2 août 2007) et le G29 (*Avis 4/2007 adopté le 20 juin, sur le concept de données à caractère personnel,* WP 136) considèrent par exemple que l'adresse IP est une donnée à caractère personnel. A l'inverse, dans deux décisions, respectivement en date des 27 avril 2007 et 15 mai 2007, la Cour d'appel de Paris a jugé, dans le cadre d'un téléchargement illicite d'œuvres musicales, que l'adresse IP (Internet Protocol) de l'internaute ayant procédé au téléchargement ne constituait pas une donnée à caractère personnel donnant lieu à déclaration préalable. Voir dans le même sens que la Cour d'appel, la décision de la High Court of Ireland (*EMI Records & Ors -v- Eircom Ltd*, 16/04/2010).

[110] Une légende apparaît alors sous l'image, indiquant le prénom et le nom de la personne « taguée », et faisant apparaître un cadre autour du visage de celle-ci.

[111] Dans un sens large par exemple, le G29 a estimé que « les données constituées par des sons et des images méritent, à ce titre, d'être reconnues comme des données à caractère personnel, dans la mesure où elles peuvent représenter des informations sur une personne physique » *Avis 4/2007* du G29 du 20 juin 2007, *sur le concept de données à caractère personnel*, WP 136, p. 8).

développement et la mise à disposition de logiciels de reconnaissance faciale. Concrètement cette fonctionnalité utilise la technologie biométrique pour reconnaitre automatiquement les visages et ainsi suggérer des noms pour identifier les nouvelles photos chargées sur le réseau social. Facebook a récemment mis en ligne un tel dispositif (depuis début juin). Les utilisateurs peuvent toutefois choisir de désactiver cette fonction s'ils le souhaitent.

Un autre exemple est celui de la fonctionnalité *Like*, sur Facebook. Ce bouton permet à un utilisateur d'indiquer une affection particulière pour toute information (un lien, un groupe, une image, un commentaire, une vidéo, un statut de profil, ses sites préférés, etc.). Certains sites extérieurs au réseau ont même intégré à leurs pages la fonction *Like*, afin de permettre à l'utilisateur d'indiquer qu'il apprécie tel ou tel site[112]. En soi, l'action d' « aimer » ne permet pas d'identifier directement une personne, elle permet cependant, lorsqu'elle est croisée avec les autres informations que l'utilisateur a « aimées» de dresser une cartographie très précise des centres d'intérêts de la personne et, le cas échéant, d'utiliser cette cartographie à des fins publicitaires.

En tout état de cause, tout étant sujet à interprétation, il reviendra au juge, ou au législateur, au cas par cas, de préciser ce qui peut être considéré ou non comme une donnée à caractère personnel sur un réseau social. En réalité, un des éléments les plus problématiques dans la mise en œuvre du droit à l'oubli numérique sur ces réseaux est l'identification du responsable de traitement.

b. La dichotomie responsable de traitement / sous-traitant peu pertinente sur les réseaux sociaux :

Deux figures sont évoquées traditionnellement dans la Loi du 6 janvier 1978, qui transpose la Directive de 1995, pour appréhender la personne qui prend en charge un traitement de données : le responsable de traitement, et le sous-traitant.

[112] A ce sujet, Le Monde rapporte qu'un Land allemand a jugé illégal le bouton "J'aime" de Facebook. Thilo Weichert, employé de l'autorité de protection de la vie privée du Schleswig-Holstein, dans le nord de l'Allemagne, a en effet estimé que le système du réseau social collectait illégalement les données des internautes, et a accordé jusqu'à la fin du mois de septembre aux éditeurs de sites qui ont intégré le bouton "J'aime", pour le retirer de leurs pages, sous peine de se voir infliger une amende de 50 000 euros (LeMonde.fr : « Le bouton "J'aime" de Facebook critiqué par les autorités allemandes » 22.08.11, 12h31 - Mis à jour le 23.08.11 à 16h25).

Selon l'article 3 de la loi du 6 janvier 1978, le responsable de traitement est, « sauf désignation expresse par les dispositions législatives ou réglementaires relatives [au]traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ». Si toutefois le traitement intervient « pour l'exercice d'activités exclusivement personnelles » (article 2§1), le responsable n'est pas soumis aux exigences de la loi : il bénéficie de ce qu'on appelle l'« exemption domestique ».

La loi prévoit en outre la possibilité de sous-traiter un traitement de données à caractère personnel. Ainsi, l'article 35§2 définit comme sous-traitant « toute personne traitant des données à caractère personnel pour le compte du responsable du traitement ». Au sens de ladite loi, un sous-traitant n'a pas la maîtrise des finalités et des moyens du traitement. En conséquence, un traitement sous-traité reste sous la responsabilité de l'organisme qui a décidé de faire appel à un sous-traitant. Il n'a d'obligations que celles de sécurité et de confidentialité.

Cette vision traditionnelle de la sous-traitance sur internet trouve cependant ses limites avec l'apparition récente d'un phénomène dont la définition précise est encore sujette à débat : le « Cloud computing ». Cette expression, traduite en français par « informatique en nuage », renvoie selon la CNIL à « la forme la plus évoluée d'externalisation, dans laquelle le client ou l'utilisateur dispose d'un service en ligne dont l'administration et la gestion opérationnelle sont effectuées par un sous-traitant (externe ou interne)[113] ». Il s'agit-là d'une définition large, qui a vocation à prendre en compte les réalités extrêmement diverses que peut recouvrir le Cloud computing[114].

D'après la CNIL, les services en ligne ainsi proposés possèdent des caractéristiques communes : une facturation à la demande, une disponibilité quasi-immédiate des ressources, une grande simplicité d'utilisation, un faible coût, et souvent l'ignorance du client quant à la localisation des données[115]. On distingue généralement les clouds privés (fermés, et créés spécifiquement pour le client), des clouds publics (ouverts, qui proposent un service auquel le client peut souscrire mais qui n'ont pas été créés spécifiquement à sa demande).

---

[113] Définition proposée par le service expertise de la Cnil, disponible à l'adresse suivante : http://www.cnil.fr/la-cnil/nos-defis/innovation-et-expertise/cloud-computing/.

[114] Pour une illustration de la difficulté de définir le Cloud computing, voir l'article du Wall Street Journal du 26 mars 2009, « The Internet Industry is on a Cloud – Whatever that may mean ».

[115] CNIL, *op.cit*.

Les réseaux sociaux semblent rentrer dans cette dernière catégorie. Ces plates-formes de communication en ligne peuvent en effet être assimilée à un service en ligne (dans un sens large) ouvert au public, dont l'objet et de permettre « à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs »[116]. Ainsi, la prestation offerte consiste à externaliser le réseau social de l'individu vers le « nuage Internet ». On retrouve également d'autres caractéristiques du Cloud computing dégagées par la Cnil : la simplicité des interfaces, la disposition immédiate des ressources (toutes les informations publiées par l'utilisateur), et même la rémunération du service, qui serait la diffusion de publicité en ligne, ciblée ou non.

Si l'on appliquait la traditionnelle dichotomie responsable de traitement / sous-traitant au phénomène du Cloud computing, et plus spécifiquement aux réseaux sociaux, on en arriverait à la conclusion suivante :

- L'utilisateur, en s'inscrivant sur le réseau social, détermine bien la finalité (se créer un réseau de contact) et les moyens du traitement (la création d'un réseau par l'intermédiaire de l'interface et des outils proposés par le réseau). Il est donc responsable de traitement.
- Toutefois l'utilisateur, agissant la plupart du temps à titre personnel, tombe sous le coup de l'exemption domestique, et les dispositions des législations en matière de protection des données ne lui sont pas applicables.
- Quant au fournisseur de service, en tant que sous-traitant, il n'aura comme unique responsabilité que celle d'assurer la sécurité et le respect des engagements qu'il a conclu avec le responsable (article 35 de la loi du 6 janvier 1978).

Selon cette logique, l'utilisateur serait considéré comme responsable de traitement, mais exempt de sa responsabilité car agissant dans un cadre personnel. Quant au fournisseur de SRS, en tant que sous-traitant, il ne serait pas non plus responsable de la mise en œuvre des droits et obligations prévus dans les textes relatifs à la protection des données. En d'autres termes, il n'y aurait pas de responsable, ce qui aurait pour effet d'annihiler l'effectivité des droits et obligations garantis par la loi du 6 janvier 1978.

[116] *Avis du G29, 5/2009, op.cit.*

Par ailleurs, on constate que les réseaux sociaux, se réservent parfois le droit de modifier unilatéralement et à tout moment les conditions générales d'utilisation du réseau. On se retrouverait donc dans la situation absurde selon laquelle le sous-traitant se réserverait le droit de modifier unilatéralement la relation contractuelle qui l'unit à son client.

Toutes ces incohérences révèlent la non pertinence de la traditionnelle dichotomie responsable de traitement/sous-traitant au regard du Cloud computing et des réseaux sociaux. En réalité, la difficulté tient au fait que sur ces réseaux, le « sous-traitant » a un pouvoir considérable sur l'information que lui est transmise, et que l'utilisateur du réseau n'a qu'une maîtrise limitée de l'information qu'il y publie. Il est difficile pour ce dernier de savoir où celle-ci est traitée, et stockée, ni de quelle manière elle est exploitée. Par conséquent, il paraît choquant qu'un fournisseur de SRS ne soit soumis à aucune obligation autre que celle de sécurité et de confidentialité, qui incombe traditionnellement au sous-traitant selon la loi Informatique et Libertés.

Inversement, il apparaît difficile de considérer que le fournisseur de SRS est de façon permanente responsable du traitement. En effet, il se borne parfois à mettre à la disposition de l'utilisateur un outil et à conserver les données des utilisateurs sur ses serveurs, sans pour autant les exploiter. Pour prendre un exemple concret, dans le cas de la mise à disposition par Facebook d'un outil de reconnaissance faciale, il conviendrait de rechercher si Facebook utilise ou non lui-même cet outil pour dresser des profils d'utilisateurs, voire de personnes non membres, notamment à des fins de prospection commerciale, ou s'il se borne à fournir cet outil aux utilisateurs qui l'exploitent, eux, à des fins personnelles.

On pourrait songer à une coresponsabilité de l'utilisateur et du fournisseur de SRS. Mais cette hypothèse reviendrait à un aménagement en trompe-l'œil. En effet, l'utilisateur bénéficiant de « l'exemption domestique », (donc non responsable en pratique) la coresponsabilité se commue en une responsabilité classique et unique du fournisseur de SRS.

En définitive, l'application de la notion de responsable de traitement aux fournisseurs de SRS reste nécessaire, mais pour des questions d'opportunité. Le critère de la qualification devient celui de la maîtrise de l'information : même si l'utilisateur détermine les finalités et les moyens du traitement, c'est le fournisseur de SRS qui a la

maîtrise réelle de l'information, et qui décide unilatéralement des conditions d'utilisation de l'outil qu'il propose au public. Il devrait donc être responsable de la mise en œuvre des droits relatifs à la protection des données, et notamment du droit à l'oubli numérique.

Il apparaît donc que l'effectivité du droit à l'oubli numérique est altérée par l'imprécision et parfois la non-pertinence des textes le consacrant. Tout est donc matière à interprétation, à l'heure où le contentieux relatif aux réseaux sociaux en France est encore peu développé. L'effectivité du droit à l'oubli numérique est en outre compliquée par une mise en œuvre contrastée de ce dernier.

B. Une mise en œuvre contrastée

Le droit à l'oubli numérique, si sa mise en œuvre optimale telle que préconisée par le G29 pose des problèmes en termes d'interprétation, peut toutefois faire l'objet d'une tentative de systématisation. L'analyse révèle que ce droit peut être appliqué, mais de manière contrastée : entre les différentes personnes fondées à invoquer leur droit à l'oubli numérique d'autre part (2), et entre les différents réseaux sociaux d'autre part (2).

1. L'application contrastée du droit à l'oubli numérique sur les réseaux sociaux en fonction du sujet de l'information

Il convient de distinguer, dans l'invocation et la mise en œuvre du droit à l'oubli numérique, les personnes qui sont membres du réseau social (a), et celles qui sont extérieures au réseau (b). On prendra ici pour hypothèse que les législations européenne et/ou française sont applicables *ratione loci*, et que les fournisseurs de SRS sont responsables de traitement.

a. Le droit à l'oubli numérique des utilisateurs du réseau social

Là encore deux cas de figure peuvent se présenter, qui entraînent chacun une application différente du droit à l'oubli numérique sur le réseau social. L'utilisateur du réseau peut en effet souhaiter que soient « oubliées » les informations qu'il a lui-même divulguées, mais aussi celles qu'un autre utilisateur a mis en ligne.

Les informations divulguées par l'utilisateur lui-même. En tenant compte de tous les développements précédents, il est possible d'identifier un droit à l'oubli des données associées au compte, ainsi que des données publiées dans le cadre de l'activité sur le réseau.

En ce qui concerne les données associées au compte : en théorie, seul le fournisseur de SRS a accès aux données d'identification associées au compte de l'utilisateur. C'est donc le fournisseur de SRS qui a la responsabilité de la mise en œuvre du droit à l'oubli numérique de l'utilisateur. Ce dernier bénéficie en principe d'un droit à la péremption des données d'identification après la suppression de son compte, ou lors de la modification de ces données. Le fournisseur de SRS doit néanmoins conserver certaines données pendant une période d'un an (décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne). Il n'est en outre pas exclu que l'écoulement des délais de prescription soit considéré comme une durée de conservation « nécessaire », afin de permettre aux fournisseurs de SRS de se prémunir contre d'éventuels litiges. A l'issue de ces délais, l'utilisateur disposerait en principe d'un droit à l'effacement, c'est-à-dire à la disparition effective du compte (qui peut se faire par l'anonymisation des données), dans les archives du fournisseur de SRS.

A ce sujet, le G29 a estimé que lorsque l'utilisateur supprime lui-même son compte, toutes les données qui sont associées au compte doivent alors être effacées. Seules les données pour lesquelles les textes imposent la conservation à des fins spécifiques (sécuritaires notamment)[117] pourraient être conservées. Le G29 a également recommandé que le fournisseur de SRS ne conserve pas les données d'identification des utilisateurs suspendus (afin de s'assurer que ceux-ci ne pourront pas se reconnecter) au-delà d'un un an[118].

Une autre question est celle de « l'oubli » des comptes inactifs et abandonnés. Le sujet a fait l'objet de nombreux débats. Faut-il supprimer un compte inactif ? Et quand ? Peut-on considérer qu'un compte constitue un ensemble de données périmées dont il serait possible de demander l'effacement au sens de la

[117] G29, Avis 5/2009, *op., cit*.., p. 11.

[118] *Ibid*.

loi du 6 Janvier 1978 ? Le problème est que par définition, l'utilisateur d'un compte inactif a cessé de s'intéresser à ce compte, et n'en demande pas la suppression. Ainsi, il est difficile d'identifier une limitation de durée claire qui impose aux réseaux sociaux la suppression d'un compte et des données associées au-delà d'une certaine période d'inactivité d'un utilisateur. D'ailleurs, les réseaux sociaux en pratique ne mettent pas en place de politique officielle de suppression des comptes inactifs. La loi française et la directive européenne n'imposent pas non plus une telle suppression. Le G29 a cependant estimé que de telles politiques devaient être mises en place[119].

En ce qui concerne les données publiées sur le réseau : A l'égard du fournisseur de SRS responsable du traitement, ou d'un fournisseur d'application, l'utilisateur bénéficie en principe d'un droit à la péremption des données à caractère personnel après la suppression de ces données. Le fournisseur de SRS ne semble pas avoir d'obligation légale de conserver ces données[120]. Le fournisseur de SRS a donc l'obligation de supprimer ces données. C'est d'ailleurs ce qu'a affirmé le G29 dans son avis de 2009[121]. Mais là encore, en pratique, se pose la question de l'extinction des délais de prescription, et de la conservation des données par les réseaux pour des raisons de sécurité.

L'utilisateur bénéficie également en principe d'un droit à l'oubli numérique envers tout autre utilisateur agissant à des fins non personnelles, donc agissant en tant que responsable de traitement (il peut s'agir par exemple d'un cabinet de recrutement ayant créé un compte sur le réseau et traitant les données de ses contacts dans le cadre de son activité professionnelle). S'il est informé de l'intention de procéder au traitement, l'utilisateur concerné pourrait aussi exercer son droit d'opposition, celui-ci ayant vocation à s'exercer avant le traitement, afin d'empêcher qu'il y soit procédé.

---

[119] *G29, Avis 5/2009*, *op., cit.*, p. 11, et proposition 14.

[120] En effet celles-ci n'étant pas des données d'identifications au même titre que les données associées à la création du compte, elles ne semblent pas rentrer pas dans le cadre du décret du 25 février 2011 qui prévoit la conservation pendant un an de certaines données.

[121] *Ibid.*

Les informations publiées par un utilisateur tiers. La mise en œuvre du droit à l'oubli vis-à-vis d'un utilisateur tiers n'est en théorie pas possible. L'utilisateur agit dans le cadre de sa liberté d'expression, ou de la liberté de la presse.

En ce qui concerne le contenu licite publié par l'utilisateur tiers : L'utilisateur concerné par les informations publiées sur le réseau ne dispose pas d'un droit à l'oubli numérique général sur l'information publiée par l'utilisateur tiers, qui bénéficie de « l'exemption domestique », et agit dans le cadre du droit à la liberté d'expression.

En ce qui concerne le contenu illicite publié par l'utilisateur tiers : Selon la distinction opérée en première partie de la présente étude, l'utilisateur dispose d'un droit au retrait du contenu illicite publié par l'utilisateur tiers. Ce droit s'exerce non pas selon la loi du 6 janvier 1978, mais selon la LCEN du 6 août 2004, ou la loi Hadopi II[122].

b. Le droit à l'oubli numérique des personnes non membres du réseau social

Les personnes non membres du réseau social ont, de la même manière que les membres, un droit au retrait du contenu illicite publié, le cas échéant, par les utilisateurs du réseau, qui s'exerce auprès du fournisseur de SRS. Elles ne bénéficient pas en revanche d'un droit à l'oubli numérique quant aux données à caractère personnel les concernant publiées par les utilisateurs dès lors que le contenu est licite (non diffamatoire, ne portant pas atteinte à la vie privée de l'individu, ne constituant ni une injure ni une menace, mention d'une condamnation judiciaire ayant fait l'objet d'une réhabilitation, etc.).

En revanche, les personnes non membres du réseau devraient pouvoir s'opposer (en usant de leur droit d'opposition) à ce que le fournisseur de SRS exploite les informations les concernant publiées par les membres à des fins commerciales (dès lors qu'il s'agit de données à caractère personnel). Concrètement, il s'agit par exemple de s'opposer à ce que

[122] *Op., cit.*

le fournisseur SRS établisse des profils de personnes extérieures à des fins de prospection commerciale, pour lui-même, ou pour des régies publicitaires.

2. Le contraste dans la mise en œuvre du droit à l'oubli par les différents réseaux sociaux

Ce contraste peut être identifié dans la pratique des différends réseaux sociaux (a). Il convient également de revenir sur les problèmes que pose le contraste dans l'applicabilité *ratione loci* du droit à l'oubli numérique (b).

a. Le contraste dans l'application du droit à l'oubli numérique

Il est rare de trouver dans les Conditions générales d'utilisation d'un réseau social la mention aux droits qui constituent le un droit à l'oubli numérique, tel qu'il est mentionné dans les législations européenne et française.

Seuls quelques réseaux, en France, reprennent le libellé de la loi « Informatique et Libertés ». Ainsi les réseaux Copainsdavant et Famicity indiquent dans leurs CGU qu'en application de la loi du 6 janvier 1978, les membres ont « un droit d'accès, de modification et de suppression des données personnelles qu'ils ont déposées sur le site[123] ». Certains réseaux peuvent également prévoir, sans reprendre ces droits, les modalités de suppression des données à la désinscription de l'utilisateur. En ce sens, les CGU du réseau Viadeo par exemple, prévoient que « dans les quarante-huit heures suivant cette désinscription, qui implique la résiliation du Contrat, toutes les données concernant le Membre seront effacées des bases de données d'APVO et le Membre n'aura plus accès au Site ni au Service[124] ».

D'autres réseaux en revanche, tel Facebook, n'indiquent pas clairement les politiques de la société en matière de durée de conservation des données, et de droit des utilisateurs à obtenir la suppression de certaines données.

---

[123] Point 2 al 2 des CGU du réseau Copainsdavant, http://copainsdavant.linternaute.com/charte/. Dans le même sens, voir les CGU du réseau Famicity, http://www.famicity.com/conditions-utilisation-de-famicity.

[124] Conditions d'Utilisation du site Web « www.viadeo.com » et du service correspondant, point 6.1.1, http://www.viadeo.com/downloads/cgv/cgu_fr.pdf. Voir également les CGU des réseaux Copainsdavant et Famicity, *op., cit*.

Les réseaux sociaux ont par ailleurs des politiques assez diverses en ce qui concerne la présentation par défaut des paramètres de confidentialité. Cela a pourtant son importance dans la mise en œuvre du droit à l'oubli numérique. En effet, plus l'individu ouvre son profil au public, plus l'information qu'il y publie est susceptible d'être diffusée et reprise par ses contacts. L'utilisateur perd alors la maîtrise de son information, et rend tout exercice de son droit à l'oubli illusoire. Le G29 a donc recommandé que les réseaux sociaux adoptent par défaut des paramètres de sécurité restreints[125], cela notamment afin de protéger les mineurs présents sur ces réseaux qui sont parfois peut conscients des conséquences que peut avoir l'ouverture de son profil à tout public. Cette recommandation est toutefois peu suivie en pratique, et de nombreux réseaux ont des paramètres de sécurité « ouverts » par défaut. Ainsi, la Commission européenne a révélé dans un communiqué de presse du 21 juin 2011 que sur quatorze réseaux examinés, seuls deux sites de socialisation prévoyaient par défaut la protection des profils privés des mineurs, soit Bebo et MySpace, et quatre sites seulement (Bebo, MySpace, Netlog et SchuelerVZ) garantissaient par défaut que les mineurs ne peuvent être contactés que par leurs amis[126].

b. *Le contraste dans l'applicabilité* ratione loci *du droit à l'oubli numérique*

Il a été constaté plus haut qu'il était possible d'étendre le champ d'application des législations européenne et/ou française à tous les réseaux, quel que soit leur lieu d'établissement (hors Union européenne, ou dans l'Union), notamment en adoptant une approche extensive de la notion de « moyen de traitement », conjuguée à l'inopposabilité des clauses éventuelles désignant comme applicable un droit autre que le droit européen.

Des arguments ont été avancés en ce sens. D'un point de vue juridique, et théorique, l'opportunité d'une application extensive des législations européennes en matière de protection des données se justifie par l'idée que tout ressortissant de l'Union doit pouvoir bénéficier des droits fondamentaux que ces textes garantissent, et notamment du droit à l'oubli numérique. L'idée est donc que la loi ne s'appliquerait pas *ratione loci*, mais plutôt *ratione personae*.

[125] Avis du G29 sur les réseaux sociaux, *op., cit.*

[126] Communiqué de presse de la Commission européenne du 21 juin 2011: « Stratégie numérique : seuls deux sites de socialisation prévoient par défaut la protection des profils privés des mineurs », IP/11/762.

Du strict point de vue du droit international privé classique, une telle approche pourrait être jugée excessive. Il est effet raisonnable de penser que les critères de rattachement prévus par les législations européennes n'ont pas vocation à être trop étirés. C'est d'ailleurs l'idée qu'exprime le G29, pourtant très progressiste en matière d'application de la Directive 95/46/CE, en estimant qu'il « n'est pas souhaitable que les règles de protection des données s'appliquent en définitive à des situations qui n'étaient pas destinées à être couvertes par ces règles et pour lesquelles le législateur ne les a pas conçues[127] ».

L'idée pose aussi de nombreuses difficultés d'un point de vue technique. Il faut prendre garde à ne pas tomber dans la caricature des réseaux sociaux, et de ne leur prêter pour seule intention, lorsqu'ils déclarent n'être pas soumis au droit européen, que celle de se soustraire à des textes trop protecteurs des utilisateurs, et donc trop contraignants. En effet, il y a aussi dans le choix de ces réseaux une véritable question pratique. Si chaque législation nationale était étendue à tous les réseaux sociaux existants, ces réseaux se verraient obliger d'appliquer autant de droits qu'il y aurait d'Etats sur le territoire desquels ils offrent un service de réseautage social.

D'une manière plus générale, entendre de manière très extensive la notion de moyens de traitement peut conduire à des résultats étonnants. En effet, selon cette logique, un site Internet brésilien basé au Brésil qui s'adresserait à un public brésilien en portugais pourrait être soumis au droit français dès lors qu'un seul utilisateur basé en France ferait usage de ce site Internet (du fait de l'installation d'un cookie sur l'ordinateur de cet utilisateur français lors d'un achat effectué sur ce site par exemple).

En réalité, ces problèmes de droit applicable, pour les réseaux sociaux situés hors de l'Union européenne, sont les témoins d'une problématique beaucoup plus vaste qui affecte le droit international privé en général. Ce dernier en effet, a vocation à arbitrer des conflits de lois dans l'espace, de part et d'autre des frontières réelles des Etats souverains. Or précisément, la révolution numérique, avec l'avènement de l'Internet, bouleverse profondément ce paradigme. La notion de frontière est remise en question. L'information circule désormais dans un espace nouveau, un « cyberespace[128] », qui serait « constitué,

[127] *G29, avis du 20 juin 2007*, op, cit.,p.5.

[128] Le terme « cyberespace » a été popularisé par William Gibson en 1984 dans son roman de science-fiction, *Neuromancer* (William GIBSON, *Neuromancer*, New York : Ace Books, 2004, 371 p.).

d'une part, de personnes de tous les pays, de toutes cultures et de toutes langues, de tous âges, de toutes professions, qui offrent et demandent des informations et, d'autre part, d'un réseau mondial d'ordinateurs interconnectés grâce aux infrastructures de télécommunications qui permettent de traiter et transmettre sous forme numérique les informations offertes et demandée[129]».

Dans ce « cyberespace » – sauf à avoir une mainmise absolue sur le système d'accès à l'Internet – les Etats ne peuvent réguler les flux qui circulent à travers leur territoire. Le droit international privé est donc bien en peine de fournir des solutions satisfaisantes dès lors que les législations prévoient en matière informatique un critère de rattachement territorial. Ce critère se justifie dès lors que des actes ou des activités ont lieu dans des endroits géographiquement différents. Or, à l'heure du cyberespace, si les parties à une relation peuvent se situer sur des territoires différents, leur action se situe sur un seul et même espace : l'Internet. Dès lors, un cadre juridique fondé sur un critère de rattachement territorial risque d'être inopérant lorsque la population qu'il entend protéger recourt à des services offerts par des prestataires étrangers.

La structure du « cyberespace » invite donc à une réflexion profonde sur le droit international en général, et sur la notion de souveraineté plus particulièrement. Celle-ci, sur l'Internet, trouve en effet ses limites lorsqu'elle est rapportée à la notion de frontière et de territoire. Elle doit peut-être désormais se tourner davantage vers la notion de personne. C'est d'ailleurs la position qu'a adopté le G29, en préconisant, pour le droit européen de la protection des données, la reconnaissance d'un critère de rattachement fondé sur « le ciblage des personnes » ou « l'approche axée sur le service»[130]. Selon ce critère, « le fait qu'un responsable du traitement collecte des données à caractère personnel dans le cadre de services explicitement accessibles ou destinés aux résidents de l'UE[131] » pourrait être déterminé par un faisceau d'indice, et entraînerait l'application de la législation européenne.

---

[129] Teresa FUENTES-CAMACHO, « L'UNESCO et le droit du cyber Espace » in *Les dimensions internationales du droit du cyberespace*, Ed. Unesco, 2000, Economica, Coll Droit du cyberespace, 284 p.

[130] *G29, Avis 8/2010 sur le droit applicable,* adopté le 16 décembre 2010, WP 179. Le G29 souligne notamment dans cet avis que le critère du « ciblage des personnes » est applicable dans certains autres domaines du droit, notamment le droit de la consommation.

[131] *Ibid*.

Quoiqu'il en soit, la pression des autorités de protection des données, et les attentes des utilisateurs des réseaux sociaux rendent aujourd'hui de plus en plus contestable la position des réseaux qui refusent catégoriquement l'application du droit européen et/ou du droit français. Ainsi par exemple, Facebook, qui se considérait soumis au droit californien, semble s'orienter, pour ce qui est du public européen, vers une reconnaissance du droit européen de la protection des données, du fait du rôle de plus en plus important joué par la société Facebook Irlande. Dès lors en vertu du critère de rattachement principal de la Directive 95/46/CE, la loi Irlandaise s'appliquerait, car Facebook serait considéré comme établi sur le sol irlandais. En revanche, pour l'application des législations des autres Etats membres de l'Union, le problème sera toujours de savoir quel rôle jouent les différentes entités de la société, telle Facebook France (dont Facebook conteste qu'il s'agit d'un établissement), et si Facebook recourt ou non à des moyens de traitement sur ces autres Etats.

Il apparaît donc que le droit à l'oubli numérique a une effectivité limitée sur les réseaux sociaux, en raison de la terminologie imprécise et peu pertinente des législations relatives à la protection des données, mais aussi en raison des contrastes qui existent dans sa mise en œuvre, en particulier au niveau de l'applicabilité *ratione loci* du droit. Par ailleurs, la circulation des informations sur le réseau et, parfois, leur indexation sur les moteurs de recherche, entraîne une perte de pouvoir de leur sujet sur celles-ci, et prive de portée toute velléité d' « oubli ».

La mise en œuvre effective du droit à l'oubli sur les réseaux sociaux suppose alors de repenser ce droit.

II. Propositions pour une meilleure effectivité du droit à l'oubli numérique

Des actions juridiques peuvent être envisagées pour une meilleure effectivité du droit à l'oubli numérique (A), ainsi que des actions extra juridiques (B).

A. Les actions juridiques : vers une internationalisation du droit à l'oubli numérique ?

Il peut être utile de renforcer et d'harmoniser les législations nationales (1). Mais surtout, le droit à l'oubli numérique ne saurait être effectif sans faire l'objet d'une véritable internationalisation (2).

1. Le renforcement et l'harmonisation des législations nationales

Pour l'instant, les législations des Etats de l'Union européennes s'alignent en principe sur les textes existants à l'échelle communautaire, telle que la Directive 95/46/CE. Par ailleurs, il a été vu que la révision prochaine de la Directive 95/46/CE envisage de renforcer les droits qui précèdent l'exercice du droit à l'oubli numérique (droit d'accès, droit d'opposition, information préalable, etc.), voire de consacrer un droit à l'oubli numérique. Il y a donc un véritable effort de renforcement du droit et d'harmonisation qui s'opère à l'échelle européenne.

Il pourrait également être envisagé de renforcer, à l'échelle européenne, les pouvoirs de contrôle et de sanction des différentes autorités de protection des données, afin de garantir une réelle mise en œuvre du droit à l'oubli numérique.

Le problème porte davantage sur le décalage qui peut exister entre les législations européennes et les autres législations. Dans le cadre des réseaux sociaux, il s'agit notamment du décalage entre les législations européennes et américaines. Or, on constate aux Etats-Unis un mouvement actuel vers un renforcement du droit de la protection des données. Ainsi, un projet de loi a été déposé devant le congrès par les sénateurs McCain et Kerry en avril 2011. Ce texte institue une charte des bonnes pratiques ayant pour objectif d'obliger les entreprises à obtenir l'accord explicite de l'internaute avant d'installer des cookies. On y trouve l'expression d'un certain droit à l'oubli. En effet, le texte prévoit en

sa section 301 « Data minimization » au point (2) (ii) qu'il est possible de conserver des informations pour une durée « raisonnable au regard de la nature du service proposé[132] ». De nombreuses associations ont cependant refusé de soutenir le texte en estimant qu'il n'allait pas assez loin (Center for Digital Democracy, Consumer Action, Consumer Watchdog, Privacy Rights Clearinghouse et Privacy Times[133]). Dans le même sens, un projet de loi déposé récemment devant le Sénat de Californie s'est donné pour objectif d'obliger les entreprises californiennes à mettre à disposition des utilisateurs une option permettant de refuser que leurs données personnelles soient enregistrées et exploitées, et d'interdire à ces sociétés de « vendre, partager, ou transférer » les informations personnelles de leurs utilisateurs ou clients[134]. Mais là encore le projet a rencontré une opposition déterminée de la part des sociétés concernées. Enfin, toujours en Californie, un projet de loi a été proposé par la sénatrice Ellen Corbett, intitulé *Social Networking Privacy Act*, ayant pour objectif de protéger les mineurs sur les réseaux sociaux. Le texte vise à donner aux parents un contrôle sur les données publiées sur le compte des enfants mineurs, qui pourraient demander au fournisseur de SRS de retirer certains contenus sous 48h[135].

Ces projets témoignent d'une volonté de répondre aux enjeux qui existent en matière de protection des données. Ils ne consacrent cependant pas réellement un droit à l'oubli numérique sur les réseaux sociaux. Par ailleurs, il n'est absolument pas certain que si un tel droit était consacré, il soit garanti de la même manière qu'en Europe. La question continuerait donc de se poser quant à l'applicabilité du droit européen aux réseaux sociaux établis hors de l'Union européenne visant un public européen. L'internationalisation du droit semble donc plus propice à une protection large des utilisateurs.

---

[132] Mr. KERRY and Mr. MCCAIN. *Bill To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, and for other purposes*. 112TH Congress, 1ST Session, BAG11284. Citation originale : It is possible to « (2) retain covered information for only such duration as (ii) if such service is ongoing [...] is reasonable for the ongoing nature of the service».

[133] Voir pour une explication, http://www.zdnet.fr/actualites/usa-democrates-et-republicains-proposent-une-loi-sur-les-donnees-privees-39759943.htm.

[134] Senate Bill, No. 761 Introduced by Senator Lowenthal, February 18, 2011, http://info.sen.ca.gov/pub/11-12/bill/sen/sb_0751-0800/sb_761_bill_20110425_amended_sen_v96.pdf.

[135] SENATE BILL No. 242, Introduced by Senator Corbett, February 9, 2011. *An act to add Part 2.7 (commencing with Section 60) to Division 1 of the Civil Code, relating to privacy.* http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0201-0250/sb_242_bill_20110209_introduced.pdf.

2. La nécessaire internationalisation du droit à l'oubli numérique

L'internationalisation du droit à l'oubli numérique passerait, dans sa configuration la plus aboutie, par une consécration explicite de ce droit dans un instrument juridique contraignant. On est cependant loin d'un tel résultat. Au demeurant, il est fort peu probable qu'un instrument international reprenne la terminologie « droit à l'oubli », tant celle-ci peine à faire l'objet d'un consensus. En revanche, des efforts ont été faits récemment pour une reconnaissance à l'échelle internationale des principes qui sous-tendent ce droit, à savoir la péremption des données, et la possibilité de voir ses données effacées au-delà d'un certain temps.

L'OCDE a ainsi récemment publié un communiqué dans lequel elle estime que « les gouvernements, le secteur privé, la communauté technique de l'Internet et la société civile devraient tous œuvrer ensemble pour donner aux individus les moyens d'un contrôle approprié et effectif sur les informations reçues et les données à caractère personnel divulguées, notamment par des initiatives de sensibilisation des internautes et des campagnes pour la maîtrise du numérique[136] ».

En ce qui concerne plus précisément les réseaux sociaux, l'Union européenne a élaboré en 2009 des « principes de l'UE pour des réseaux sociaux plus sûrs[137] », auxquels les réseaux sociaux souscrivent par le biais d'une déclaration[138]. Les objectifs de ces accords sont de favoriser sur les réseaux la mise en place d'un système de signalement des abus, de recommander pour les mineurs un paramétrage restreint des profils par défaut, et une bonne information des utilisateurs mineurs du réseau (lisibilité et accessibilité des options de paramétrage et de l'information).

Par ailleurs, en mars 2008, le groupe de travail international sur la protection des données dans les télécommunications a adopté un avis intitulé « Mémorandum de Rome ». Pour le mémorandum toutefois, « la notion d'oubli n'existe pas sur internet ». Le groupe de travail préfère donc analyser les risques d'atteinte à la vie privée et à la sécurité posés

[136] Communiqué sur les principes applicables à la politique de l'internet réunion à haut niveau de l'OCDE sur l'économie internet, 28-29 juin 2011. http://www.oecd.org/dataoecd/33/36/48387644.pdf.

[137] Bruxelles, le 10 février 2009, IP/09/232. « Socialisation sur internet: accord entre les grands sites par l'entremise de la Commission ».

[138] Parmi les signataires, on trouve : Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google/YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klaza.pl, Netlog, One.lt, Skyrock, StudiVZ, Sulake/Habbo Hotel, Yahoo!Europe, and Zap.lu.

par les réseaux sociaux et fournit des lignes directrices aux régulateurs, fournisseurs et utilisateurs, pour un meilleur contrôle de l'information[139].

Il faut encore ajouter à ces travaux la résolution de la conférence internationale des commissaires à la protection des données qui a été organisée à Strasbourg en octobre 2008[140], ainsi que l'avis du 12 juin 2009 du G29 relatif aux réseaux sociaux[141]. Ces deux textes recommandent un paramétrage par défaut favorable à la vie privée, ainsi qu'une suppression des profils d'utilisateur à la résiliation du compte. Le G29 préconise également une durée de conservation des données limitée. Il est vrai que certains de ces travaux ont reçu un large écho, tel l'avis de 2009 du G29. Les CNIL européennes, en l'absence de texte spécifique aux réseaux sociaux, font de l'avis de 2005 une doctrine qu'elles appliquent quotidiennement dans leurs décisions, leurs conseils, leurs délibérations, voire dans d'éventuelles mises en demeure ou sanctions.

Il n'en reste pas moins que ces différents travaux, s'ils témoignent d'une dynamique sans précédent en faveur de l'internationalisation du droit de la protection des données, n'ont pas valeur contraignante.

Par conséquent, de nombreuses organisations et autorités de protection des données tentent depuis plusieurs années de mettre en commun leurs efforts afin d'élaborer des standards internationaux de protection de la vie privée et, à terme, de mettre au point un instrument international ayant une valeur juridique contraignante[142].

Dans ces travaux, si le droit à l'oubli numérique n'est pas explicitement mentionné, il est néanmoins pris en compte. Ainsi, lors de la 31ème Conférence mondiale des Commissaires à la protection des données, qui s'est tenue en novembre 2009 à Madrid, les

---

[139] Groupe de travail sur les communications électroniques, Report and Guidance on Privacy in Social Network Services - « Rome Memorandum » 4 mars 2008. Citation originale : « The notion of oblivion does not exist on the Internet. Data, once published, may stay there literally forever ». http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491.

[140] 30ème Conférence des commissaires à la protection des données et à la vie privée Strasbourg, 15-17 octobre 2008, Résolution sur la protection de la vie privée dans les services de réseaux sociaux. http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_fr.pdf.

[141] *Op., cit.*

[142] Pour des exemples, voir notamment la recommandation de l'OCDE du 12 juin 2007 relative à la coopération transfrontière dans l'application des législations protégeant la vie privée, les conférences régionales de l'Unesco en 2005 (Asie-Pacifique) et 2007 (Europe) qui soulignent le caractère prioritaire de la protection des données, ou encore les nombreux avis du groupe de l'article 29 de l'Union européenne, ainsi que les différentes Conférences mondiales des Commissaires à la protection des données.

autorités de protection des données représentant plus de 40 pays ont adopté des standards internationaux relatifs à la protection de la vie privée et des données personnelles, qui reprennent les principes qui sous-tendent le droit à l'oubli numérique. L'article 9.2 prévoit en effet que « la Personne Responsable devra limiter la durée de conservation des Données Personnelles traitées au minimum nécessaire. Ainsi, lorsque les Données Personnelles ne sont plus nécessaires pour atteindre les finalités qui ont légitimé leur Traitement, elles doivent être effacées ou rendue anonymes. » La « Personne Concernée » a d'ailleurs le droit de « demander à la Personne Responsable l'effacement […] de Données Personnelles qui pourraient être […] non nécessaires ou excessives » (article 17)[143].

Plus récemment, en octobre 2010, la 32ème Conférence mondiale des autorités de protection des données a permis l'adoption d'une résolution, proposée par la CNIL française, prévoyant la convocation d'une Conférence intergouvernementale, au plus tard en 2012, aux fins d'adopter un instrument international contraignant sur le respect de la vie privée et de la protection des données personnelles[144]. La Déclaration finale du G8 qui s'est tenu les 26 et 27 mai 2011 à Deauville[145] a intégré cette préoccupation en appelant « à la définition d'approches communes tenant compte des cadres juridiques nationaux, qui soient fondées sur les droits de l'homme et protègent les données à caractère personnel, tout en permettant les transferts légitimes de données » (article II. 16).

L'ONU elle non plus n'est pas étrangère aux enjeux de la de protection des données. Un rapport récent de Franck La Rue a en effet estimé que si le droit d'accès à Internet était un droit humain qui ne pouvait faire l'objet de restrictions, il était également fondamental de préserver la vie privée des internautes[146]. A ce sujet, le rapporteur spécial indique que la protection des données personnelles constitue un aspect particulier du droit au respect de la vie privée. Il ajoute que toute personne devrait pouvoir accéder à ses

[143] 31ème Conférence des commissaires à la protection des données et à la vie privée Madrid, Résolution sur des normes internationales de vie privée Espagne, 4-6 novembre 2009.

[144] 32e Conférence mondiale des commissaires à la protection des données et de la vie privée Jérusalem, 27-29 octobre 2010 résolution appelant à la convocation d'une conférence intergouvernementale aux fins d'adopter un instrument international contraignant sur le respect de la vie privée et la protection des données personnelles.

[145] Déclaration finale du G8 de Deauville 26-27 mai 2011. Source : http://www.g20-g8.com/g8-g20/g8/francais/en-direct/actualites/un-nouvel-elan-pour-la-liberte-et-la-democratie.1313.html.

[146] LA RUE, Franck. Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté 'expression et d'opinion, 16 mai 2011, A/HRC/17/27, §53-59.

données, être informée de la manière dont elles sont traitées, et pouvoir consentir à ce qu'une entité publique ou privée les traite ou non[147].

Il est donc permis de penser qu'un processus est désormais lancé, vers l'élaboration d'un véritable instrument juridique contraignant, à l'échelle internationale. Il est fort probable que la consécration d'un principe général de protection de la vie privée soit dans ce cas consacré. Le droit à l'oubli numérique pourrait implicitement y avoir sa place, si les principes de droit à la péremption des données et de droit à l'effacement des données périmées étaient repris.

Le droit cependant, ne peut à lui seul garantir l'effectivité d'un droit à l'oubli numérique. Il doit nécessairement s'accompagner d'actions extra juridiques.

B. Les actions extra juridiques

La mise en œuvre du droit à l'oubli numérique doit passer par son intégration technique au sein des plateformes de réseautage social (1), mais aussi par une prise de conscience des enjeux de l'oubli à l'échelle individuelle (2).

1. L'internalisation du droit à l'oubli numérique par les SRS : la « privacy by design »

La « privacy by design » est un concept à mi-chemin entre le droit et la technique. L'idée n'est pas nouvelle. On la trouve dès 1990 dans plusieurs publications du professeur Ann Cavoukian[148]. Il s'agissait de démontrer la nécessité d'une prise en compte de la vie privée dans le développement de nouvelles technologies dès la conception du produit, tout en faisant comprendre aux entreprises que la vie privée pouvait devenir un avantage concurrentiel.

---

[147] *Ibid*.

[148] « Privacy Protection Makes Good Business Sense » publié par le Commissariat à la Protection des données d'Ontario en Octobre 1995. http://www.ontla.on.ca/library/repository/mon/1000/10294138.htm et « Privacy: The Key to Electronic Commerce » publié par le Commissariat à la Protection des données d'Ontario en avril 1998 disponible à l'adresse http://www.ipc.on.ca/images/Resources/e-comm.pdf.

Ce concept, souvent traduit en français par « la prise en compte de la vie privée dès la conception », a été repris par les défenseurs de la vie privée, par les autorités de protection des données, et par certaines entreprises[149]. Le concept de « privacy by design » n'est d'ailleurs pas étranger aux textes européens relatifs à la protection des données. Le considérant 46 de la directive 95/46/CE prévoit par exemple que « la protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en œuvre du traitement ».

En ce qui concerne les réseaux sociaux, et la mise en œuvre du droit à l'oubli numérique, la « prise en compte de la vie privée dès la conception » du produit reviendrait à s'assurer que les services offerts à l'utilisateur permettent, dès leur mise à disposition du public, l'exercice effectif du droit. C'est notamment ce qu'a exprimé le G29, dans son avis de 2009, il insiste sur la nécessité de prévoir une politique claire en matière de durée de conservation des données. Il recommande également des paramètres de confidentialité respectueux de la vie privée par défaut, et la mise en place d'un « bureau des réclamations ». Enfin, il estime que les SRS devraient « recommander à leurs utilisateurs de ne pas mettre en ligne des images ou des informations concernant d'autres personnes sans le consentement de celles-ci ». Tous ces paramètres permettraient alors une meilleure maîtrise de l'information tout au long de sa présence sur le réseau, et rendraient, au moment voulu, sa disparition effective possible.

Certains auteurs ont également proposé des solutions techniques pour permettre l'oubli à l'ère numérique. Ainsi, le chercheur Viktor Mayer Schönberger propose de réfléchir à la mise en place d'un système de dates d'expiration qui serait couplées à chaque donnée. A l'image d'un titre donné à un document lors de son enregistrement sur un ordinateur, chaque individu aurait l'obligation de définir une durée de conservation avant de pouvoir mettre à disposition une information le concernant[150]. Cela permettrait donc au

[149] Par exemple, Marc MOSSE, Directeur des affaires publiques et juridiques, a insisté sur l'importance de la *privacy by desig* lors de la conférence sur le droit à l'oubli numérique à Sciences-Po Paris du 12 novembre 2009 (*op., cit.*).

[150] V.MAYER SCHÖNBERGER, *op., cit.* p 140 et s. L'auteur précise que le recours à des dates d'expiration pourrait être mis en œuvre par le recours à des méta-informations (ce sont les informations associées la donnée en question, tel que la date de création, le titre, etc.), et par une législation imposant l'installation d'un logiciel adapté dans tous les ordinateurs et autres supports numériques, afin que ces méta-informations relatives à la date d'expiration de l'information puissent être lues et mises en œuvre.

sujet de l'information de décider de la péremption à venir de ses informations. L'auteur ajoute que le législateur pourrait en outre fixer des plafonds pour les dates d'expiration de certaines informations particulièrement sensibles, que l'individu ne serait pas nécessairement en mesure d'apprécier.

Il n'en reste pas moins que sur Internet, toute action juridique ou technique ne saurait suffire sans l'action volontaire et responsable du sujet de l'information.

2. La responsabilité du sujet de l'information

Le pouvoir décisionnel des individus sur leur information n'est pas négligeable. Pour Viktor Mayer Schönberger, la conscience des enjeux de l'oubli à l'ère numérique pourrait conduire à une modification des comportements individuels. Ainsi tout internaute pourrait limiter la quantité d'information qu'il divulgue sur la Toile, et donc limiter les informations qui ne pourraient être « oubliées ». Cela pourrait se faire soit par un phénomène de rétention (publier moins), soit par un phénomène de précaution (installation sur les navigateurs d'extensions permettant de crypter les données, ou de limiter la publicité ciblée, etc.). Le problème sur les réseaux sociaux est que les utilisateurs ne sont pas nécessairement en position de négocier avec les fournisseurs de SRS, et ne sont pas forcément prêts à sacrifier les avantages qu'ils retirent du partage de leurs données. Néanmoins, tout individu sur l'Internet et particulièrement sur les réseaux sociaux, est un consommateur, au sens économique du terme. Il recourt à un service, et exige de ce dernier certains standards de qualités. Par conséquent, si l'ensemble des consommateurs formulaient des exigences élevées en termes de vie privée, ou formulaient le souhait de voir leur droit à l'oubli numérique respecté, il est probable que les SRS adaptent leurs politiques et les modalités d'utilisation de leurs plateformes. La sensibilisation des individus, et notamment des jeunes, peut donc constituer une clé de la mise en œuvre sur les réseaux sociaux. Plus ceux-ci seraient conscients des enjeux de la protection des données, plus ils formuleraient des exigences élevées en la matière, auxquelles devraient nécessairement répondre les réseaux sociaux, afin de préserver avec leurs utilisateurs une relation de confiance.

CONCLUSION

Force est de constater, à l'issue de la présente étude que, s'il est possible de dégager les grands axes d'un droit à l'oubli numérique sur les réseaux sociaux, la mise en œuvre de ce dernier pose davantage de questions qu'elle n'offre de réponses. Il est donc souhaitable que la révision de la directive 95/46/CE précise, renforce, voire consacre un droit à l'oubli numérique.

L'analyse a par ailleurs révélé les faiblesses d'un droit qui se voudrait restreint au seul territoire d'un Etat. Les nouvelles frontières du cyberespace – ou plutôt l'absence de frontières – invitent à se demander si le droit de la protection des données ne doit pas s'appliquer en fonction du public ciblé, plutôt qu'en fonction de la localisation d'un moyen de traitement ou d'un établissement procédant à un traitement. Une autre solution pourrait encore être l'internationalisation du droit à l'oubli numérique.

Plus généralement, les difficultés de mise en œuvre de ce droit invitent à s'interroger sur la pertinence d'une action qui se voudrait essentiellement juridique. Le rôle du juriste n'est plus simplement de bâtir un arsenal juridique qui soit le plus protecteur possible. Il doit désormais intégrer dans son approche l'indispensable sensibilisation des internautes, et prendre en compte la part d'autorégulation qui s'opère sur les réseaux sociaux. Le droit ne serait plus qu'un instrument parmi d'autres de la protection des libertés fondamentales et des droits de l'homme sur l'Internet.

L'univers numérique bouleverse la représentation traditionnelle des espaces et du droit. Chez l'homme, il bouleverse son pouvoir sur l'information, et son rapport au temps. Ainsi, la place croissante qu'occupent les technologies numériques dans la vie des nouvelles générations devrait mener à terme à un ajustement cognitif[151]. Il s'agirait alors d'apprendre à ne plus oublier, ou plutôt, à ne plus souffrir de l'absence d'oubli. C'est-à-dire que la révolution numérique, selon Jeffrey Rosen, nous invite peut-être à réinventer les notions d'empathie et de pardon[152].

[151] V.MAYER SCHÖNBERGER: *Delete: The virtue of forgetting in the digital age*, *Op., cit.*

[152] ROSEN, Jeffrey. « The web means the end of forgetting », publié dans *The New York Times* le 21 juillet 2010 (15 pages). Source : http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

BIBLIOGRAPHIE

1. OUVRAGES

BELLEIL, Arnaud. *E-Privacy : Le marché des données personnelles : protection de la vie privée à l'âge d'Internet.* Paris : Dunod, 2001, 202 p.

BENSOUSSAN, Alain. *L'informatique et le droit*, Paris :Hermès, 1994, 694 p., p. 466.

BERGSON, Henri. *L'énergie spirituelle. Essais et conférences. (1919).* Paris : P.U.F., 1967, 214 p.

FRAYSSE, Emmanuel. *Facebook, Twitter et le web social, les nouvelles opportunités de business: stratégies, marketing , meilleures pratiques* » , Agence Kawa, Numilog, 2e éd., 2011, 346 pp.

FREUD, Sigmund. « Nouvelles remarques sur les psychonévroses de défense », in *Névrose, psychose et perversion.* Paris : P.U.F., 1973, 306 p.

GIBSON, William. *Neuromancer,* New York : Ace Books, 2004, 371 p.

KAPLAN, Daniel. *Informatique libertés, identités*, Ed Fyp., 2010, 142p.

NIBOYET, Marie-Laure et DE GEOUFFRE DE LA PRADELLE, Géraud. *Droit international privé,* Ed. Lextenso, L.G.D.J., 2009. 792 p.

NIETZSCHE, Friedrich. *Considérations intempestivesII, 1, (1874).*Trad. BIANQUIS, Geneviève. Paris : Aubier-Montaigne, 1976, 361 p.

NIETZSCHE, Friedrich. *Généalogie de la morale.* Paris : Flammarion, 1996, 278 p.

RICOEUR, Paul. *La mémoire, l'histoire, l'oubli.* Paris : Seuil, 2003, 689 p.

SCHÖNBERGER, Viktor Mayer. *Delete: The Virtue of Forgetting in the Digital Age.* Princeton University Press, 2009, 237 p.

SPARROW, Andrew. *The law of virtual worlds and Internet social networks* Burlington : Gower, 2010, 249 p.

UNESCO. *Les dimensions internationales du droit du cyberespace,* Ed. Unesco, 2000, Economica, Coll Droit du cyberespace, 284 pp

2. TRAVAUX ET PUBLICATIONS

a) Thèse

ROQUES-BONNET, Marie-Charlotte. *Le droit peut-il ignorer la révolution numérique ?* Paris : Michalon 2010, 607 p.

b) Articles de périodiques

BALAGUE, Christine. « Les entreprises ne peuvent plus passer à côté des réseaux sociaux », *Fréquence Banque*, n°75 (Janvier-Février 2011), p.3.

BATTISTI Michèle. « Le droit à l'oubli numérique, un droit à construire », *Sciences de l'information*, n° 1 (Février 2010), p.24-25.

BENSOUSSAN, Alain. « Le "droit à l'oubli" sur Internet », *Gazette du Palais*, n° 36-37 (Vendredi 5, samedi 6 février 2010) p.3.

BOYER, Joël. « Droit à l'oubli, droit de suppression, droit de suite : la loi Informatique et libertés doit-elle arbitrer la liberté d'expression ? » *Légicom* (Paris), 46. La presse en ligne : Actes du Forum Légipresse du 7 octobre 2010 / Claude Weill / Paris : Victoires éditions – 2011.

CAPRIOLI, Arnaud. « Lieu d'archivage des données et loi applicable – Impunité de Google en matière de vie privée sur le territoire français ». *Revue Communication – Commerce électronique*, octobre 2008, p. 44.

CAVOUKIAN, Ann et EMAN, Khaled El. « Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy ». *Information and Privacy Commissioner*, Ontario, Canada, June 2011, 19 pp. Disponible à l'adresse : http://www.ipc.on.ca/images/Resources/anonymization.pdf.

COSTES, Lionel. « Une charte sur le "droit à l'oubli numérique" », *Revue Lamy Droit de l'immatériel*, n°65, novembre 2010, p.3.

DECAUX, Emmanuel. « La protection de la vie privée au regard des données informatiques », Revue électronique *Droits fondamentaux*, n°7, janvier 2008 – décembre 2009, p. 3.

DESGENS-PASANAU, Guillaume. « Le droit à l'oubli existe-t-il sur internet ? », *Expertises des systèmes d'information*, n° 343 (janvier 2010), p.11-12.

FOREST, David. « "Là-bas si j'y suis" ou les mirages du droit à l'oubli numérique », *Revue Lamy Droit de l'immatériel*, n° 56, Janvier 2010, p.90.

FRAYSSINET, Jean. « Le pseudo droit à l'oubli appliqué à la presse », *Légipresse*, n°276, Octobre 2010, p.273-279.

FROCHOT, Didier. « Le droit à l'oubli numérique : nouvelle donne sur internet ? », *Archimag*, n°235 (Juin 2010), p. 42-43.

FUENTES-CAMACHO, Teresa. « L'UNESCO et le droit du cyber Espace » in *Les dimensions internationales du droit du cyberespace*, Ed. Unesco, 2000, *Economica*, Coll Droit du cyberespace, 284 p.

GAUTIER, Pierre-Yves. « Réseaux sociaux sur l'internet, données personnelles et droit de contrats », *Recueil Dalloz* 2009 p. 616.

GEFEN, Alexandre. « Appel à contribution », *Revue ¿Interrogations* , 2006, n°3. <http://www.revue-interrogations.org/fichiers/contrib6/Appel%20a%20contribution%203%20l%20oubli.pdf>.

KOSSAIFI, Christine. « L'oubli peut-il être bénéfique ? L'exemple du mythe de Léthé : une fine intuition des Grecs ». *Revue ¿Interrogations ?*, 2006, n°3, p. 43-57. <http://www.revue-interrogations.org/fichiers/57/mythe_de_lethe.pdf>.

LETTERON, Roseline. « Le droit à l'oubli », *Revue du droit public*, 1996, T. CV, n°2, p. 385-424.

MONTREYRE, Richard « *Affaire Bénédicte S.*, Variations sur la détermination de la loi applicable à Google », *Revue Expertises*, août septembre 2008, p.296-300.

MOREAU, François. « Communautés en ligne et réseaux sociaux : des colosses aux pieds d'argile ? », *Les cahiers de l'Arcep* n° 2 (Avril-Mai-Juin 2010), p.11.

PIOTET, Dominique. « Comment les réseaux sociaux changent notre vie », *Esprit* (Juillet 2011), p.82-95

TEXIER, Bruno. « Réseaux sociaux pro : l'info au bord de l'obésité », *Archimag*, n°235 (Juin 2010), p.17-19.

THIERACHE, Corinne. « Le droit à l'oubli numérique : un essai qui reste à transformer » *Revue Lamy Droit de l'immatériel*, n°67 (Janvier 2011), p.6-10.

TÜRK, Alex. « Réseaux sociaux et vie privée », *ENA hors les murs*, n°400 (Avril 2010), p.10-12.

3. TRAITES, CONVENTIONS, DIRECTIVES, LOIS

a) Droit français

Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel portant transposition de la directive 95/46/CE.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) .

Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel portant transposition de la directive 95/46/CE.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) .

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après loi « Informatique et Libertés ».

Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, JORF n°0050 du 1 mars 2011.

Proposition de loi n°331 *visant à mieux* garantir *le droit à la* vie privée *à l'heure du* numérique, présentée Par M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER, Sénateurs, déposée au Sénat le 6 novembre 2009.

Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche, signée à Paris, le 13 octobre 2010, sous l'impulsion de Madame Nathalie KOSCIUSKO-MORIZET, alors Secrétaire d'Etat chargée de la prospective et du développement de l'économie numérique.

b) Droit américain

SENATE BILL, No. 761 Introduced by Senator Lowenthal, February 18, 2011, http://info.sen.ca.gov/pub/11-12/bill/sen/sb_0751-0800/sb_761_bill_20110425_amended_sen_v96.pdf**.**

SENATE BILL No. 242, Introduced by Senator Corbett, February 9, 2011. *An act to add Part 2.7 (commencing with Section 60) to Division 1 of the Civil Code, relating to privacy.* http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0201-0250/sb_242_bill_20110209_introduced.pdf.

Mr. KERRY and Mr. MCCAIN. Bill To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, and for other purposes. 112TH Congress, 1ST Session, BAG11284.

b) Conseil de l'Europe

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractères personnel, Conseil de l'Europe, STCE n° 108, entrée en vigueur le 05 mai 1985.

Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, 1950.

c) Union européenne

Charte des droits fondamentaux de l'Union européenne (2000/C 364/01).

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) *Journal officiel n° L 201* du 31/07/2002 p. 37-47.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données *Journal officiel n° L 281* du 23/11/1995 p. 31-50.

Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs**.**

Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I) *Journal officiel n° L 177 du 04/07/2008 p. 0006 – 0016*.

Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale *Journal officiel n° L 012 du 16/01/2001 p. 0001 - 0023*.

4. JURISPRUDENCE

Conseil constitutionnel, 2004-496 DC, 10 juin 2004.

Conseil constitutionnel, n° 2003-475 DC du 24 juillet 2003.

Conseil constitutionnel, n°1999-421 DC du 16 décembre 1999.

CASS. 1re civ., 3 déc. 1991, RCDIP 1992, 340 note H. GAUDEMET-TALLON.

CASS., Civ. 1re, 20 novembre 1990, *Mme Monanges c. Kern.*

CASS., 21 juin 1950, *Messageries maritimes*, Grands arrêts de la jurisprudence française de droit international privé (5ème éd., 2006), arrêt n° 22, p. 194.

COUR D'APPEL de Paris, 13e chambre, section A, 15 mai 2007, Monsieur H. S. c/ Ministère Public, Société civile des producteurs phonographiques.

COUR D'APPEL de Paris, 13e chambre, section B, 27 avril 2007, Monsieur G. c/ Ministère Public, Société civile des producteurs phonographiques.

TGI Montpellier ord. réf., Marie C. / Google France et Inc, 28 octobre 2010.

TGI Paris, ord. réf., *H. Giraud c./ Facebook France*, 13 avril 2010.

TGI Paris Ordonnance de référé 12 octobre 2009 Mme X, Société L. & Com / Jean-Hervé C.

TGI Paris, ord. réf., 25 juin 2009.

TGI Paris ord. réf., *Bénédicte S / Google Inc.*, Google France, 14 avril 2008.

TGI Paris, 20 avril 1983, *Mme Filipacchi c. Soc. Cogedipresse*.

T.G.I., Seine, 14 octobre 1965, *Mme Segret c. Soc. Rome-Paris Films*, note de GERARD LYON-CAEN, *J.C.P*, 1966.II.14482.

Allemagne, Cour constitutionnelle fédérale allemande (Bundesverfassungsgerichsthof), 15 décembre 1983 (BVGE 65, 1.). Commentaires de POULLET Yves et ROUVROY Antoinette.

Etats-Unis, US Federal District Court of Los Angeles *Ticketmaster v. Tickets.com*,2000 WL 525390 (C.D.Cal.,2000), 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. 2000).

Etats-Unis, Superior Court Of California, Mendoza v. AOL, (2000), County of Alameda, dept. No. 22.

5. RAPPORTS ET AVIS

LA RUE, Franck. Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'expression et d'opinion, A/HRC/17/27, 16 mai 2011.

DINANT, Jean-Marc ; PEREZ ASINARI, Maria Veronica ; POULET, Yves ; DE TERWANGNE, Cécile. « L'autodétermination informationnelle à l'ère de l'Internet », Rapport pour le Comité consultatif de la convention pour la protection des personnes à

l'égard du traitement automatisé des données à caractères personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

THYRAUD, Jacques Rapport n° 72 (1977-1978), fait au nom de la commission des lois, déposé le 10 novembre 1977.

DÉTRAIGNE, Yves et ESCOFFIER, Anne-Marie. « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information ». Rapport d'information n° 441 (2008-2009), fait au nom de la commission des lois, déposé le 27 mai 2009.

CNIL. 30ème rapport d'activités, 2009.

G29, WP 163, avis 5/2009 sur les réseaux sociaux en ligne, adopté le 5 juin 2009.

G29, WP 136, avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007.

G29, WP 148, Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, adopté le 4 avril 2008.

G29, WP 179, Avis 8/2010 sur le droit applicable, adopté le 16 décembre 2010.

8. COMMUNICATIONS ET ARTICLES JOURNALISTIQUES

Communication de la Commission au Parlement européen, au Conseil, au Comite économique et social européen et au Comité des régions : «Une approche globale de la protection des données à caractère personnel dans l'Union européenne» ; Bruxelles, le 4.11.2010 COM(2010) 609 final.

Discours de Mme REDING, Membre de la Commission européenne responsable de la Société de l'Information et des Médias à propos de l'Initiative « Futur de l'Internet» du Conseil Européen de Lisbonne (2 février 2009): «l 'Internet du futur: l'Europe doit jouer un rôle majeur ».

CHASTAND Jean-Baptiste La délicate question du droit à l'oubli sur Internet / *in Le Monde, (12/11/2009)* .

DUTON Jean-Christophe et BECHT Virginie: « Le droit à l'oubli numérique : un vide juridique ? », Le journal du Net, 24/02/2010.

EUDES Yves « Le droit à l'oubli, un "droit fondamental » in Le Monde > (01/04/2009) (Archives) .

LEMONDE.FR : « Le bouton "J'aime" de Facebook critiqué par les autorités allemandes » 22.08.11, 12h31 - Mis à jour le 23.08.11 à 16h25.
http://www.lemonde.fr/technologies/article/2009/11/12/la-delicate-question-du-droit-a-l-oubli-sur-internet_1266457_651865.html.

WALL STREET JOURNAL du 26 mars 2009, « The Internet Industry is on a Cloud – Whatever that may mean ».
Source : http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

8. RESOLUTIONS ET COMMUNIQUES

Communiqué sur les principes applicables à la politique de l'internet réunion à haut niveau de l'OCDE sur l'économie internet, 28-29 juin 2011. http://www.oecd.org/dataoecd/33/36/48387644.pdf.

Résolution appelant à la convocation d'une conférence intergouvernementale aux fins d'adopter un instrument international contraignant sur le respect de la vie privée et la protection des données personnelles. 32e Conférence mondiale des commissaires à la protection des données et de la vie privée Jérusalem, 27-29 octobre 2010. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/2010-conf_itlee_resolution_projet_FR.pdf.

Résolution sur des normes internationales de vie privée Espagne, 4-6 novembre 2009. 31ème Conférence des commissaires à la protection des données et à la vie privée Madrid, http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Con fitle_Israel_2010_resolution_standard_FR.pdf.

TABLE DETAILLEE