LE DROIT : UN OUTIL DE RÉGULATION DU CYBERESPACE ?

Le cas du droit à l'oubli numérique

Rhéa Edde

L'Harmattan | « L'Homme & la Société »

2018/1 n° 206 | pages 69 à 94

ISSN 0018-4306
ISBN 9782343148854

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-l-homme-et-la-societe-2018-1-page-69.htm

Pour citer cet article :

Rhéa Edde, « Le droit : un outil de régulation du cyberespace ? Le cas du droit à l'oubli numérique », *L'Homme & la Société* 2018/1 (n° 206), p. 69-94.
DOI 10.3917/lhs.206.0069

Le droit : un outil de régulation du cyberespace ?

Le cas du droit à l'oubli numérique

Rhéa EDDE
Dicen-IDF[1] (EA 7339), UFR PHILLIA[2]
Université Paris Nanterre

Le droit est une discipline vivante, évolutive et qui s'adapte à son environnement. Le nouvel écosystème économique mondial, marqué par le numérique, est également un lieu d'interactions humaines. La mobilisation de normes juridiques pour l'encadrer constitue un défi pour le droit.

À l'heure du *big data*, tout est devenu traces, les données personnelles sont désormais une des ressources essentielles de l'économie numérique. Elles sont un enjeu stratégique pour les États comme pour les entreprises. Outre la question de leur exploitation, leur numérisation et leurs possibilités infinies de stockage et de conservation donnent à la mémoire digitale un pouvoir démesuré en annihilant la faculté d'oubli. Cet effet d'éternité de la mémoire interroge l'oubli en tant que problématique philosophique et psychologique.

Ce bouleversement de grande ampleur engendré par Internet questionne l'articulation du droit face aux mutations du numérique. Comment naissent et se développent de nouveaux droits, et en particulier le droit à l'oubli numérique, en réponse à un besoin social de régulation de nouvelles pratiques ?

La conception originaire d'Internet est celle d'un espace de liberté ouvert, où l'intervention du droit est délicate. Toutefois, la nécessité de

1 Dispositifs d'information et de Communication à l'Ère numérique – Paris Île-de-France.

2 UFR de Philosophie, information-communication, langage, littérature, arts du spectacle (PHILLIA) ; Bât. L, 200 avenue de la République, 92001 Nanterre.

contrôler l'utilisation économique des traces de l'internaute et la protection des droits de l'homme impose-t-elle de faire de l'oubli numérique un droit ? Pourquoi, comment est né et s'est développé ce « nouveau droit », le droit à l'oubli numérique ? Quel compromis le droit opère-t-il entre la protection des droits de l'Homme et notamment le respect de la vie privée et de la liberté d'expression, les intérêts économiques des acteurs du marché et les mutations de la société ? Dans une économie mondialisée et digitale, le droit national, qui s'inscrit dans le cadre normatif de la souveraineté de l'État, a-t-il encore une utilité ?

Cet article se propose d'examiner les raisons et les modalités de naissance du droit à l'oubli numérique. Il explore ensuite le contenu de ce droit subjectif (qui vise uniquement les données personnelles) en droit français et européen, pour déterminer comment il s'articule avec le respect de la vie privée et de la liberté d'expression. Enfin, cet article analyse la mise en œuvre de ce nouveau droit qui reflète les interrogations relatives à la transformation des législations nationales et à leur efficience au sein du cyberespace. En effet, la mondialisation induit une déconnexion des règles de toute territorialité, Internet est un espace global par essence qui ne connaît pas les frontières étatiques. Ces enjeux sont donc au centre de la réflexion juridique contemporaine.

À l'origine du droit à l'oubli numérique : le passage de l'Internet pour tous au *big data* et ses enjeux

Traces et identité numérique

La création originelle d'Internet est appréhendée comme un moyen d'échanger librement et gratuitement des informations. Les valeurs d'Internet sont les valeurs communautaires et libertaires régnant au sein des communautés scientifiques américaines dans les années 1960 et qui ont modelé le Web (Flichy, 2001). Le Web 2.0 permet un nouvel espace d'expression aux citoyens, de création de lien social, un moyen d'entrer, de participer et de compter dans le débat public, un moyen de partager et d'acquérir des connaissances, un moyen de mettre en place des actions collectives, politiques ou non.

Le développement de l'écosystème numérique se fait de pair avec une certaine transformation de la sociabilité traditionnelle. Avec la démocratisation des usages du Web, l'omniprésence numérique est conditionnée par des utilisations variées et de nouvelles formes de sociabilité apparaissent, dans la mesure où ce média permet de multiplier

les contacts avec un grand nombre de personnes connues ou inconnues. Les réseaux sociaux en ligne s'inscrivent dans un nouveau modèle de communication et de partage qui illustre une évolution sociale et culturelle. Ils encouragent l'expression de soi et notamment de l'intimité. Les internautes n'hésitent pas à exposer leur vie sur Internet et disséminent de nombreux indices qui peuvent toucher à la sphère privée.

À chaque fois qu'un internaute noue des relations, dépose du contenu sur lui ou sur des tiers, il laisse des indices. Toute activité sur la toile engendre la création de traces. Internet est ainsi le lieu d'un nouveau type d'identité, l'identité numérique. Cette dernière est une « collection de traces » (Merzeau, 2009 : 26). Elle est construite à partir de très nombreuses sources : des traces volontaires (création de contenus par l'internaute), des traces involontaires (issues de l'usage d'Internet à savoir l'adresse IP et les cookies) et hors du contrôle de l'internaute et de traces subies (informations laissées par des tiers sur l'internaute). Multisources, l'identité est créée à la fois par l'internaute et à partir d'actions d'autres personnes.

L'identité numérique sur le Web 2.0 se décompose en trois composantes (Georges, 2008) : l'identité déclarative, l'identité agissante et l'identité calculée. L'identité déclarative, renseignée directement par l'internaute, est la description de la personne par elle-même. Autour de ce noyau de l'identité s'intègrent les identités agissante et calculée. L'identité agissante a pris son essor avec le Web 2.0 et est renseignée indirectement par les activités communautaires et personnelles de l'internaute sur la toile. Quant à l'identité calculée, elle est issue d'un traitement de l'identité agissante par le système.

Décortiquant également l'identité numérique sur les réseaux sociaux, Philippe Mouron la décompose aussi en trois dimensions. Une dimension technique qui transparaît à travers les données de connexion de l'internaute. Une dimension réelle qui touche à l'ensemble des éléments subjectifs de la vie privée de la personne (identifiants, image, géolocalisation…). Ces données rendues publiques brouillent les frontières entre sphère publique et sphère privée. Enfin, une dimension intellectuelle qui est composée de « toutes les productions de l'esprit que crée l'individu pour élaborer une identité fictive » (Mouron, 2012 : 220).

En conséquence, l'identité numérique est complexe, plurielle et spécifique. Elle est modelée en partie par l'internaute et peut se disjoindre de son propriétaire, les données pouvant circuler indépendamment de sa volonté. Cela la différencie nettement de l'identité civile qui est, quant à elle, organisée par les autorités nationales et indissociable de l'individu.

Avec le *big data* et les capacités techniques d'archivage massif, les données et traces constitutives de l'identité numérique prennent un nouveau tournant.

Big data *et archivage massif des traces numériques : entre exploitation économique, surveillance et mémoire universelle*

Aujourd'hui, sous l'impulsion de plusieurs innovations, Internet a franchi une nouvelle étape, celle du *big data*. Cette nouvelle ère numérique entraîne un changement de paradigme qui se caractérise par la croissance exponentielle de données, leur circulation, leur stockage sous forme digitale, leur traitement et leur agrégation par des outils d'analyses spécifiques, les algorithmes, et leur potentialité de valorisation.

> La révolution digitale est le passage d'une société industrielle à une société de service. Elle est basée sur les données. […] À l'instar de l'évolution industrielle, l'évolution de l'ère digitale repose sur la capacité à toujours mieux exploiter les informations existantes et à exploiter de nouvelles sources d'informations. C'est ce qu'on appelle généralement le *big data*. (Cointot & Eychenne, 2014 : 3)

Cette grande variété des données se conjugue avec leur énorme volume et la rapidité de leur circulation.

Le *big data* génère de nombreuses données personnelles et les dote d'une valeur marchande. Il s'agit de données nominatives qui permettent d'identifier une personne[3]. Toutefois, aujourd'hui, tout devient donnée personnelle : des informations dont le recoupement permet d'identifier une personne précise, une adresse IP[4], les traces informatiques exploitables grâce aux moteurs de recherche… Comme le souligne Judith Rochfeld, toute personne peut être également identifiable, « […] à partir de toutes données laissées sur le réseau ou captées par un objet connecté : tout est devenu données personnelles dès lors qu'il est possible, à partir d'une photographie, de remonter, grâce à un logiciel de reconnaissance faciale et/ou par croisement avec une autre donnée, à l'identité de la personne ; la

---

3 Selon l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite loi informatique et liberté : « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

4 Cour de cassation, 1re chambre civile, 3 novembre 2016.

navigation électronique de la personne dans un moteur de recherche (notamment les *search logs* ou mots clés qu'elle utilise) permet de l'identifier par recoupement de ses centres d'intérêts et de ses requêtes ou de son adresse IP. » (Rochfeld, 2015 : 74).

Les données personnelles, qualifiées de nouvel or noir, ont une valeur économique : ce sont des matières premières, des leviers de gains et d'opportunités et des actifs stratégiques (Chignard & Benyayer, 2015). Elles constituent un enjeu concurrentiel au cœur de l'économie numérique, de la *data driven economy*. Leur utilisation génère de nouvelles perspectives et opportunités pour tous les secteurs d'activités et reconfigure les relations de pouvoir.

Tout internaute est un consommateur et donc un client potentiel. Au sein de l'économie numérique, la gratuité est omniprésente. Mais, comment se finance cette gratuité ? La valeur marchande des données personnelles récoltées et valorisées, « cette expropriation identitaire » (Merzeau, 2009 : 27) constitue la contrepartie, selon les opérateurs qui les utilisent, de cette gratuité. Ainsi, l'échange monétaire est remplacé par la collecte de données devenant elle-même monnaie d'échange.

Comme le souligne Chris Anderson dans *Free! Entrez dans l'économie du gratuit*, « l'essor de l'économie de gratuité, ou *freeconomics*, est alimenté par les technologies de l'ère numérique » (Anderson, 2009 : 14). L'auteur recense dans son ouvrage quatre types de modèles économiques fondés sur la gratuité. Le premier modèle est celui des subventions croisées directes, dans lequel l'acquisition d'un objet incite le consommateur à en acheter un autre (par exemple l'impression de cartes de visites en ligne avec échantillon gratuit). Dans le deuxième modèle, celui du marché tripartite, le financement est assuré par la publicité (c'est le cas par exemple de YouTube, du référencement payant de Google). Le troisième modèle est celui des dons (c'est par exemple le cas de Wikipédia). Et enfin, le modèle « freemium » fusionne deux modèles : un modèle gratuit (*free*) et un modèle *premium* payant. Les utilisateurs *premium*, qui paient pour avoir des fonctionnalités que n'ont pas les utilisateurs *free*, sont ceux qui financent l'utilisation du service par ces derniers (par exemple logiciel de création en ligne).

Les chercheurs Joëlle Farchy, Cécile Méadel et Guillaume Sire décryptent, dans leur ouvrage *La Gratuité à quel prix*, le concept de gratuité numérique à l'œuvre dans trois secteurs : l'audiovisuel, la musique et le livre. Ils mettent en exergue que la circulation et l'échange de biens culturels sur Internet recouvrent des modèles économiques organisés et structurés.

> Le consommateur accède donc désormais à de multiples plateformes de contenus en ligne selon diverses logiques de réception (téléchargement ou streaming), de commercialisation (location temporaire ou vente définitive à l'acte, abonnement, etc.) ou de financement (paiement du consommateur ou gratuité totale ou partielle). Pourtant derrière une même apparence de gratuité pour l'internaute se cachent des modèles économiques fort divers dont il est possible d'établir une typologie […]. (Farchy, Méadel & Sire, 2015 : 16)

La gratuité pour l'internaute, le fait de ne pas payer des biens et des services prend ainsi différentes formes : publique (la redistribution publique), coopérative et marchande.

Par ailleurs, dans cette continuité, les économistes Jean Tirole et Jean-Charles Rochet (2003) considèrent que la gratuité est illusoire. Pour eux, la majorité, voire l'ensemble des marchés, sont des marchés bifaces *two-sided markets*. En leur sein, l'offre et la demande sont interdépendantes pour créer le marché. Ils organisent des interactions entre plusieurs catégories d'usagers où ce qui est gratuit pour les uns est en réalité payé par les autres.

Cette économie numérique, cette économie de la donnée bouleverse les rapports de force entre les acteurs. Comme l'analyse Louise Merzeau, « opérateurs, marchands, moteurs de recherche et services de renseignements en savent plus sur nos comportements numériques que nous-mêmes, car ils ont la capacité de les archiver, de les recouper et de les modéliser » (Merzeau, 2009 : 27).

Les Gafa (Google, Apple, Facebook et Amazon) maîtrisent les données de millions de personnes. Avec la collecte des données GPS et leur croisement avec les données de navigation, ils détiennent encore plus de renseignements sur les internautes. Ces géants, qui disposent d'une quantité phénoménale de données, posent des défis en matière de souveraineté numérique et mettent à mal les législations des États.

Les entreprises, elles aussi, utilisent les données des consommateurs pour analyser et/ou revendre des données personnelles afin de développer leurs services et générer de nouveaux revenus. Cela contribue à une connaissance, plus personnalisée et plus approfondie, des clients et transforme la relation des clients à la marque. Deux modèles sont à l'œuvre, selon Simon Chignard et Louis-David Benyayer (2015), dans cette économie de la donnée. D'une part, il y a le modèle biface fondé sur le troc implicite des données personnelles contre un service gratuit. D'autre part, le modèle serviciel, dont les données personnelles sont l'élément clé, et qui permet la personnalisation des services avec un bénéfice partagé entre client et entreprise.

Quant aux États, ces flux d'informations peuvent servir leurs intérêts géopolitiques ou nationaux. La surveillance des populations est possible par la récupération massive d'informations sur les individus à partir des traces numériques de leurs activités.

> En particulier, en prenant appui sur les possibilités d'enregistrement, de traçabilité et de traitement automatisé inhérents au numérique, de vastes dispositifs de surveillance, de censure et de manipulation des informations se sont également mis en place, ouvrant à des formes de contrôle sur les individus. Ces transformations s'inscrivent dans le cadre plus général du déploiement, sur le long terme, d'un « ordre sécuritaire » qui s'appuie sur l'innovation technologique. (Loveluck, 2016 : 334-335)

À l'ère du *big data*, la mémoire numérique est infinie, éternelle et mobilisable à tout moment. Internet anéantit la faculté d'oubli inhérente au temps qui passe et opère comme une mémoire permanente, illimitée, précise, non sélective, avec une facilité de conservation, de stockage, de consultation et d'exploitation notamment économique et commerciale. Cela expose l'individu « 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. » (Quillet, 2011 : 7).

En conséquence, cela pose la question centrale du maintien du contrôle de l'internaute sur ses données personnelles en ligne et leur durée de conservation.

Une étude sociologique, menée dans le cadre de la *Recherche sur le droit à l'oubli* réalisée avec le soutien de la Mission de recherche Droit et Justice (Boizard dir., 2015), analyse l'appréhension du droit à l'oubli à travers les comportements, les attitudes et les pratiques face au droit à l'oubli numérique d'un échantillon d'internautes. Elle révèle que :

> […] les individus sont conscients des conséquences de l'usage d'Internet sur la protection des données et informations les concernant mais ils font état d'une sorte de fatalisme. Cette situation peut sans doute s'expliquer par la difficulté que certains éprouvent à comprendre de manière très précise les mécanismes limitant l'usage de leurs données. Elle s'explique également par le souhait exprimé par les usagers de pouvoir continuer à bénéficier des services gratuits

> proposés en ligne parce qu'ils leur apportent des avantages. Le bénéfice de ces services justifie qu'ils acceptent certains risques liés notamment au recueil de leurs données. (Boizard dir., 2015 : 26-27)

Le *big data* et l'archivage massif, l'agencement et la modélisation des données met en lumière des risques et des enjeux importants en matière de droits de l'Homme, en particulier au regard du respect de la vie privée et de la liberté d'expression. Le *big data* signe-t-il la fin des libertés individuelles et de la sphère privée ? Face à cette situation, comment protéger l'internaute ? Comment lui redonner le pouvoir de maîtriser ses données et la gestion de ses traces ?

L'émergence du droit à l'oubli numérique comme nouveau droit des personnes

Internet, espace de liberté, « n'est pas naturellement celui du droit » comme le souligne le Conseil d'État dans son rapport *Internet et les réseaux numériques* (Conseil d'État, Thery & Falque-Pierrotin, 1998 : 6). Toutefois, d'une part, cet espace de liberté est protégé par le droit français et européen et, d'autre part, la recherche du profit par les entreprises et le contrôle des contenus par les organisations et par les États ont conduit à l'intervention de la règle de droit pour réguler le cyberespace.

L'articulation du droit à l'oubli, de la liberté d'expression, de la protection de la vie privée et de la protection des données personnelles

Internet, en tant qu'espace de liberté, est protégé par le droit français et européen avec une double perspective : liberté d'accès à Internet et liberté d'expression sur Internet.

Le droit d'accès à Internet est consacré par la législation française et européenne, mais connaît des limites. Le Conseil constitutionnel, dans sa décision n° 2009-580 du 10 juin 2009, consacre le droit d'accéder à Internet. Ce dernier résulte de la liberté d'expression. En effet, le Conseil constitutionnel considère « qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services »[5]. Quant à la Cour européenne des droits de l'Homme (CEDH), elle s'appuie sur l'article 10 de la Convention européenne

[5] Conseil constitutionnel, décision n° 2009-580, 10 juin 2009.

de sauvegarde des droits de l'Homme et des libertés fondamentales, pour, elle aussi, reconnaître un droit des internautes d'accès à Internet[6].

Toutefois, ce droit d'accès à Internet, inclus dans la liberté d'expression, n'est pas absolu. Le blocage des contenus est prévu dans certains cas par la législation française[7] et mis en œuvre par les juridictions[8]. De même, la CEDH exerce un contrôle en cas de blocage de l'accès à Internet par un État. L'arrêt CEDH, *Ahmed Yildrim c. Turquie*, 18 décembre 2012, en constitue une illustration. L'affaire concernait le blocage total de Google Sites par les autorités turques, mesure qui avait été ordonnée dans le cadre d'un contentieux pénal. Le requérant soutenait que ce blocage engendrait une censure indirecte, car il avait pour effet de verrouiller également l'accès à tous les autres sites hébergés par le serveur. En conséquence, le demandeur arguait que cette mesure, décidée dans le cadre d'une affaire pénale qui n'avait aucun rapport ni avec lui ni avec son site, avait pour résultat de l'empêcher d'accéder à son site internet. La CEDH a conclu à la violation de l'article 10 de la Convention européenne, notamment au regard des effets arbitraires de la mesure en cause.

Quant à la liberté d'expression, liberté fondamentale, elle est posée de façon globale et réaffirmée dans le cadre de ce nouveau moyen de communication qu'est Internet. La liberté d'expression est ainsi consacrée en droit international, en droit européen et en droit français. Des restrictions à la liberté d'expression sont prévues par les textes pour empêcher les atteintes à des intérêts collectifs ou aux droits des particuliers.

Plus spécifiquement, la liberté d'expression sur Internet est une application de la liberté d'expression à un nouveau support de communication. Aussi, la liberté d'expression sur Internet est un droit garanti : « la communication au public par voie électronique est libre »[9].

---

6 CEDH, 18 décembre 2012, n° 3111/10, *Ahmet Yildirim c. Turquie*.

7 C'est le cas en matière de jeux ou de paris en ligne illicites. L'Autorité de régulation des jeux en ligne (ARJEL) peut mettre en demeure le contrevenant de faire cesser l'infraction dans un délai de huit jours, faute de quoi l'ARJEL peut faire un recours en référé pour obtenir une injonction à l'égard des fournisseurs d'accès Internet pour qu'ils bloquent l'accès au site incriminé.

8 Ainsi, le Tribunal de grande instance de Paris, 3e chambre, SCPP/Orange, Free, SFR et Bouygues Télécom du 4 décembre 2014, a fait droit à la demande de la Société civile des producteurs phonographiques (SCPP) qui demandait le blocage du réseau Pirate Bay constitué des sites principaux site d'origine : thepiratebay.se et des sites de redirection pour atteinte aux droits des producteurs de phonogrammes membres de la SCPP.

9 La loi n° 2004-545 du 21 juin 2004 pour la confiance dans l'économie numérique.

Toutefois, ce droit n'est pas absolu. En effet, Internet est un nouvel outil puissant d'exercice de la liberté d'expression en raison de la facilité et de l'instantanéité de diffusion des informations à grande échelle, mais il présente des risques pour les internautes et peut être source d'abus et d'atteinte aux droits d'autrui sanctionnée par les législations française et européenne. L'intervention de la règle de droit est alors nécessaire pour limiter la diffusion de contenus illicites qui portent atteinte à la dignité de l'Homme.

Le *big data*, conjugué à la liberté d'expression, conduit à ce que d'abondantes informations soient rendues publiques sur Internet, disponibles dans le monde entier et qu'elles restent en ligne de nombreuses années après les faits et puissent porter atteinte à la vie privée (profilage, diffusion de photos ou d'informations intimes, d'informations erronées, de propos diffamatoires ou injurieux, de condamnations pénales anciennes…). Or, la protection de la vie privée, comme la liberté d'expression, est un droit fondamental consacré par l'article 9 du Code civil français : « chacun a droit au respect de sa vie privée » et par l'article 8 de la Convention européenne des droits de l'Homme.

Par ailleurs, l'essor des plateformes de réseaux sociaux en ligne a fait entrer Internet dans l'ère de la personnalisation, de la massification, de la facilité accrue de communication et d'interaction. Les informations personnelles sur la vie privée circulent librement sur le Web brouillant les frontières entre sphère publique et sphère privée. Comme le montre le sociologue Dominique Cardon dans son article « Les réseaux sociaux en ligne et l'espace public » (2010a), l'exposition exacerbée de soi est le principal ressort des réseaux sociaux. Ces derniers sont devenus le quotidien des individus, une part importante de leur sociabilité. C'est un espace où les internautes conversent, donnent leurs avis. Cette exposition de soi est un risque pour la vie privée, car les informations personnelles diffusées peuvent être consultées, réutilisées par des tiers à l'insu de leur auteur.

Ainsi, le numérique permet l'abondance et l'hétérogénéité des données personnelles collectées. La multiplication des échanges des données personnelles et leur manipulation peuvent conduire à une atteinte à la vie privée. Plus encore, l'activité des moteurs de recherche accroît ce risque. L'indexation qu'ils opèrent s'effectue en fonction du critère de pertinence et non de l'actualité des informations et selon l'algorithme du moteur de recherche, ce qui contribue à reconfigurer l'identité des personnes. Les moteurs de recherche facilitent l'accès aux informations publiées sur Internet, amplifient leur visibilité, rendent le temps élastique, la mémoire

numérique universelle et l'oubli impossible. Ce phénomène entre en opposition avec le mécanisme de la mémoire humaine. En effet, s'il n'y a pas d'identité sans mémoire, la mémoire individuelle est une réalité psychique vécue comme un phénomène présent explicitement rattaché à une réalité objective passée. L'oubli, entendu comme la disparition progressive du souvenir, constitue un mécanisme normal. Il libère l'individu du passé, et est une condition de l'action et de la création individuelle. La mémoire digitale annihile ce mécanisme.

Face à ces nouveaux contexte et enjeux, le droit traditionnel est contraint de s'adapter pour répondre aux besoins des utilisateurs. Pour protéger la vie privée, les données personnelles et faire face à une mémoire numérique illimitée et permanente, l'oubli numérique va être créé de façon artificielle et consacré comme un droit pour préserver les libertés individuelles de l'internaute. Aussi, après un long cheminement, un « nouveau droit » a émergé en droit français et européen : le droit à l'oubli numérique. Comme l'oubli ne fonctionne pas de façon naturelle sur Internet, le droit à l'oubli numérique agit comme un contrepoids indispensable à la mémoire digitale. Il tente de concilier, d'opérer un équilibre entre plusieurs droits : la protection de la vie privée, la liberté d'expression et le droit du public à l'information, la protection des données personnelles et libertés économiques.

Plus encore, face à ces enjeux mondiaux, le droit à l'oubli « doit donc être pensé de manière volontaire » (Walczak, 2012 : 124). Définir un droit à l'oubli uniquement à un niveau national est limitatif et fragile. En conséquence, une conception de ce droit à l'échelle européenne est indispensable pour le doter d'une capacité à devenir concret.

Le droit à l'oubli numérique : un renforcement des droits de la personne

La définition du droit à l'oubli est complexe. Nous l'aborderons sous le prisme du droit français et du droit européen.

Il existe des mécanismes juridiques anciens de droit à l'oubli comme l'amnistie (l'oubli officiel pénal) ou la prescription (l'oubli comme usure du temps). Le droit à l'oubli numérique diffère et comprend une dimension nouvelle, celle d'une durée de conservation limitée des données personnelles. Le droit à l'oubli numérique peut s'appréhender par sa finalité.

> Il s'agit d'écarter tout risque qu'une personne, dont des données la concernant ont été déposées sur la toile, par elle-même ou un tiers, soit durablement incommodée par l'utilisation à son insu de ces données. Et ce, quelle que soit l'ancienneté des faits ou des données se rapportant à cette personne[10].

Pour comprendre les fondements de ce nouveau droit, il faut rappeler qu'il vise plusieurs objectifs : (i) lutter contre la collecte, l'exploitation économique et commerciale des traces disséminées par les internautes, (ii) répondre à une exposition de soi et à une mise en visibilité amplifiée par les réseaux sociaux qui ont transformé l'espace public contemporain (Cardon, 2010b), (iii) limiter le caractère infini et perpétuel de la mémoire digitale.

Aussi, le droit à l'oubli numérique doit-il protéger de façon absolue la vie privée en donnant à l'internaute la maîtrise de ce qu'il laisse voir et savoir sur lui, sur Internet, ou la liberté d'expression et le droit du public à l'information doivent-ils primer ? Pour opérer un compromis entre ces deux droits fondamentaux, le droit à l'oubli numérique va s'ancrer sur deux fondements : la protection de la vie privée et la protection des données personnelles.

Le respect de la vie privée a d'abord été le cadre du droit à l'oubli. Il est protégé par différentes dispositions qui garantissent le droit au respect de la vie privée : l'article 9 du Code civil, l'article 2 de la Déclaration des droits de l'Homme et du citoyen, l'article 7 de la charte des droits fondamentaux, l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. Signalons que le Conseil constitutionnel[11] a reconnu au respect de la vie privée une valeur constitutionnelle par son rattachement au principe de la liberté individuelle, qui est une liberté constitutionnellement garantie. La Cour européenne a rappelé dans certains arrêts que « la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention »[12]. Une illustration intéressante de la connexion entre protection de la vie privée et droit à l'oubli numérique en droit français est le jugement de la 17ème chambre du tribunal de grande instance de Paris du 6 novembre 2013, *Max Mosley c. Google France*. Dans cette affaire, la société Google Inc. a été condamnée pour atteinte à la vie privée du

---

10 Définition mentionnée dans l'appel à projet de juin 2011 de la Recherche sur le Droit à l'oubli réalisée avec le soutien de la Mission de recherche Droit et Justice (Boizard dir., 2015 : 12).

11 Conseil constitutionnel, décision n° 99-416, 23 juillet 1999.

12 CEDH, 17 décembre 2009, n° 16428/05, *Gardel c. France*.

demandeur et lui a ordonné de retirer et de cesser tout affichage des images litigieuses de Max Mosley sur Google Images pendant une durée de cinq ans.

Le droit à l'oubli numérique peut également s'appréhender dans le cadre de la protection des données personnelles qui bénéficie d'une protection juridique spécifique. C'est une préoccupation ancienne de la législation française et des institutions européennes avec pour finalité la conciliation de la protection de la vie privée et la nécessité de conserver et de traiter des données.

Le texte pivot est la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite « informatique et libertés » refondue par la loi du 6 août 2004[13]. Cette dernière a été aussi modifiée pour intégrer les changements de la loi du 7 octobre 2016[14].

La loi « informatique et libertés » définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Elle concerne uniquement les personnes physiques et s'applique aux traitements automatisés et non automatisés de leurs données personnelles. Elle renforce les droits des personnes sur leurs données. Elle détaille les pouvoirs de contrôle et de sanction de la Commission nationale de l'Informatique et des Libertés (CNIL).

Avant la loi du 7 octobre 2016, le droit à l'oubli comme droit à l'effacement des données personnelles, n'était pas expressément consacré mais il se laissait entrevoir indirectement à travers différentes modalités de mise en œuvre comme l'obligation d'information à la charge du responsable de traitement, le droit d'accès[15], le droit de rectification[16] et le droit d'opposition[17].

---

13 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 et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Cette loi n° 2004-801 du 6 août 2004 prend en compte 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, et la 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.

14 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

15 Toute personne peut demander au responsable du traitement de données à caractère personnel si des données personnelles la concernent sont traitées et obtenir des informations sur le traitement et la communication sous forme accessible des données (une copie de ces données).

> Le droit au respect de la vie privée et la protection des données personnelles n'avaient pas à l'origine vocation à se rencontrer : le premier protégeait la personne dans ses relations avec les particuliers tandis que le second assurait la protection des citoyens contre l'État. […] Avec le développement d'Internet, les protections ont convergé l'une vers l'autre. Le droit à la protection des données personnelles […] sert désormais aussi à protéger la vie privée des internautes contre les pratiques intrusives. (El Badawi, 2016 : 17)

C'est la Cour de justice de l'Union européenne (CJUE) qui, la première, consacre le droit à l'oubli numérique dans son arrêt du 13 mai 2014 Google Spain[18]. En l'espèce, un citoyen espagnol se plaignait du fait qu'en tapant son nom sur le moteur de recherche Google, ce dernier affichait une liste de résultats avec des liens vers deux pages d'un quotidien espagnol datées de janvier et mars 1998, et qui annonçaient notamment une vente aux enchères immobilières organisée à la suite d'une saisie destinée à recouvrer les dettes de sécurité sociale. Le requérant faisait prévaloir que cela portait atteinte à son image et à ses affaires.

S'appuyant sur la directive n° 95/46/CE relative à la protection des données personnelles[19], la CJUE juge que le droit européen s'applique aux moteurs de recherche. Elle reconnaît que l'exploitant d'un moteur de recherche sur Internet est responsable du traitement[20] qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers.

---

16 Toute personne peut exiger que les données personnelles la concernant soient rectifiées, complétées ou mises à jour ; que soient effacées les données inexactes ou celles dont le traitement est interdit.

17 Toute personne physique 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. Le droit d'opposition à la prospection notamment commerciale est absolu et gratuit. Le droit d'opposition ne s'applique pas quand le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement.

18 CJUE, Grande chambre, 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, Affaire C-131/12.

19 Cette directive vise à protéger les libertés et droits fondamentaux des personnes physiques (droit à la vie privée notamment) lors du traitement des données à caractère personnel tout en éliminant les obstacles à la libre circulation de ces données.

20 Le responsable du traitement est la personne physique ou morale qui détermine les finalités et les moyens de toute opération (collecte, enregistrement, modification...), appliquée à des données à caractère personnel.

La CJUE aborde ensuite la question du droit à l'oubli numérique. Elle désigne l'exploitant du moteur de recherche comme celui en charge de la mise en œuvre d'un droit à l'oubli. Les résidents européens disposent d'un droit à demander le déréférencement, auprès des moteurs de recherche, de résultats en lien avec leur identité, sous réserve de certaines conditions. En pratique, le déréférencement n'efface pas l'information sur le site Internet source, mais il la supprime de l'affichage des résultats sur le moteur de recherche en cas de requête effectuée sur la seule base du nom de la personne concernée. Ce droit à l'oubli numérique doit se fonder sur un motif légitime. Ce droit à l'oubli, droit au déréférencement, vise les contenus illégitimes et inexacts. Il concerne également les contenus exacts et légitimes qui, avec l'écoulement du temps, deviennent nuisibles, des données devenues « inadéquates, non pertinentes ou excessives au regard des finalités du traitement, qu'elles ne sont pas mises à jour ou qu'elles sont conservées pendant une durée excédant celle nécessaire, à moins que leur conservation s'impose à des fins historiques, statistiques ou scientifiques (§ 92) ».

La CJUE fait ainsi prévaloir la protection de la vie privée. L'obligation de déréférencement doit primer, les droits de la personne concernée « prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à trouver ladite information lors d'une recherche portant sur le nom de cette personne (§ 97) ».

Toutefois, un juste équilibre doit être trouvé entre la protection de la vie privée et le droit d'information du public. Cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information, de sa sensibilité pour la vie privée de la personne concernée, ainsi que de l'intérêt du public à recevoir cette information. Cet intérêt peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique. Les demandes font l'objet d'une analyse au cas par cas par les moteurs de recherche. En cas de refus de la part de ces derniers, la personne concernée peut saisir l'autorité de contrôle (en France, la CNIL) ou l'autorité judiciaire pour que celles-ci effectuent les vérifications nécessaires et ordonnent à ce responsable des mesures précises.

Plusieurs arrêts ultérieurs des juridictions françaises procèdent à des condamnations dans le droit fil de l'arrêt de la CJUE de 2014[21].

---

[21] Tribunal de grande instance de Paris, ordonnance de référé du 19 décembre 2014 ; Tribunal de grande instance de Paris, ordonnance de référé du 13 mai 2016 ; Cour de cassation, 1re chambre civile, 12 mai 2016.

L'Union européenne franchit un pas supplémentaire en adoptant un nouveau règlement général sur la protection des données (RGPD)[22], entré en vigueur le 25 mai 2016 et qui sera applicable à partir du 25 mai 2018 dans tous les pays de l'Union européenne. Ce règlement constitue une évolution importante du cadre juridique de la protection des données et harmonise et régule les législations de l'Union européenne sur la question. C'est une source de sécurité juridique pour les particuliers.

> Le règlement renforce les droits des personnes et les adapte à l'ère numérique. Il conforte la place de l'individu au cœur du système juridique, technique et éthique de la protection des données en Europe. (CNIL, 2017a : 17)

Un des éléments qui a été le plus débattu lors de la préparation et l'adoption de ce règlement est la question du droit à l'oubli numérique. Dans sa version initiale, l'article 17 qui en parlait avait pour titre « droit à l'oubli numérique et à l'effacement ». Ce titre devient dans sa version finale « Droit à l'effacement ("droit à l'oubli") ».

Avec ce droit, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données personnelles la concernant, et le responsable du traitement a l'obligation d'y procéder. L'article 17 liste un nombre limité de cas où ce droit à l'effacement, ce droit à l'oubli s'applique[23].

Il est important de noter que ce droit à l'oubli numérique n'est pas absolu. Des exceptions au droit à l'oubli numérique sont mentionnées, dans le cas où le traitement est nécessaire : à l'exercice de la liberté d'expression et

---

22 Règlement nº 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

23 Les motifs sont au nombre de six :

1. les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
2. la personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ;
3. la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement ;
4. les données à caractère personnel ont fait l'objet d'un traitement illicite ;
5. les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
6. les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information.

d'information ; au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; pour des motifs d'intérêt public dans le domaine de la santé publique ; à des fins archivistiques dans l'intérêt public ; à des fins de recherche scientifique ou historique ou à des fins statistiques et enfin à la constatation, à l'exercice ou à la défense de droits en justice.

Anticipant la mise en œuvre du règlement européen sur la protection des données (RGPD), la France adopte la loi n°2016-1321 du 7 octobre 2016 sur la République numérique qui franchit un pas supplémentaire. Tout d'abord, il est intéressant de mentionner que ce texte de loi a été co-écrit avec les internautes grâce à une consultation directe menée par le Conseil national du numérique, entre octobre 2014 et février 2015. Plus de quatre mille contributions ont été recueillies, une stratégie numérique a été présentée le 18 juin 2015 par le gouvernement. Puis une consultation publique a été organisée du 26 septembre 2015 au 18 octobre 2015 sur le texte de l'avant-projet de loi. Ce processus constitue en soi une innovation.

Sur le fond et en ce qui concerne la protection des citoyens sur Internet, ce texte pose plusieurs principes : la neutralité des réseaux, la portabilité des données et le principe de loyauté des plateformes de services numériques. La loi octroie de nouveaux droits aux individus en matière de données personnelles. Les mineurs disposent désormais d'un droit à l'oubli numérique (droit à l'effacement) avec une procédure accélérée pour son exercice. Le droit à l'autodétermination informationnelle, à savoir la nécessaire maîtrise par l'individu de ses données, est affirmé et replace l'individu au cœur de la toile en le responsabilisant par rapport au contrôle de ses données.

> L'inscription de ce droit dans le droit interne français […] traduit un principe implicite, et réaffirme ainsi que la personne humaine est le centre de gravité de la législation sur la protection des données. Cela ne signifie bien sûr pas que ce droit soit illimité : il doit être concilié, dans les conditions prévues par la loi, avec l'intérêt légitime, notamment, des entreprises ou administrations qui traitent les données, ou avec l'intérêt général, par exemple en matière de sécurité publique ou en matière fiscale. Mais après des débats qui ont conduit à des interrogations sur une éventuelle « patrimonialisation » des données, il permet d'inscrire avec force que le citoyen français et européen est titulaire de droits à l'égard de ses données, quel que soit le détenteur de celles-ci, ou leur éventuel transfert. C'est parce que la donnée porte sur l'individu que celui-ci peut exercer ses droits, droits qui ne peuvent pas être cédés à un tiers ou monnayés. (CNIL, 2017a : 40)

De plus, la loi institue également un droit à la mort numérique (tout individu pourra contrôler l'usage de ses données après sa mort). Ces droits renforcent incontestablement la maîtrise des usages des données personnelles des personnes concernées.

Quelle efficience du droit à l'oubli ?

Le droit à l'oubli numérique illustre les questionnements contemporains qui agitent le droit et interroge son efficacité à l'heure du numérique. Si l'intervention du droit se justifie pour protéger les libertés individuelles, l'absence de frontières du Web, les avancées technologiques, les divergences d'avis entre les États rendent l'efficacité de ce droit délicate. Son efficience illustre les enjeux au cœur des différentes transformations, notamment numériques, que connaît cette discipline en ce début du XXI^{e} siècle. Tout d'abord, la mondialisation et le cyberespace déconnectent les droits sujets de leur territorialité. Le droit à l'oubli numérique trouve là une des principales difficultés de son effectivité. Ensuite, ce sont les acteurs économiques, et non plus les États, qui sont en charge en partie de son respect.

La déterritorialisation du droit

Le premier constat relatif à l'efficience du droit à l'oubli numérique est celui de sa portée territoriale.

Internet en sa qualité de phénomène global modifie les contours des notions juridiques et s'affranchit des frontières étatiques. Ainsi, les notions de vie privée ou de liberté d'expression ne recouvrent pas les mêmes conceptions selon les pays. À titre illustratif, la liberté d'expression dans la conception française et européenne est un droit relatif dont les abus sont sanctionnés. Le *freedom of Speech*, du premier amendement de la Constitution américaine, est un principe absolu garanti. La conception américaine est de ce fait même beaucoup plus libérale en la matière. Des différences existent aussi entre la conception française et européenne du droit au respect de la vie privée et la conception américaine du *Right to privacy*.

De plus, la mondialisation et le cyberespace remettent en cause la souveraineté des États dans l'élaboration du droit et déterritorialisent les normes juridiques. Ainsi, en ce qui concerne le droit à l'oubli numérique, signalons d'emblée un des apports importants du règlement européen sur la protection des données (RGPD) qui sera directement applicable pour tous les responsables de traitements et sous-traitants qui ont leur établissement

principal sur le territoire de l'Union européenne. À défaut d'un tel établissement, il s'appliquera aux responsables de traitements dès lors que des résidents européens seront sensiblement visés par les traitements de données mis en œuvre. Ainsi, « les acteurs mondiaux seront donc soumis au droit européen dès lors qu'ils offrent un produit ou un service à un citoyen européen, même à distance. Ce critère, dit du "ciblage", constitue une évolution profonde : désormais, la territorialité du droit européen de la protection des données se construit autour de la personne, et non plus seulement autour du territoire d'implantation des entreprises » (CNIL, 2017b : 9).

Le droit à l'oubli numérique entendu comme le droit au déréférencement pose la question essentielle de sa portée territoriale. En effet, le droit au déréférencement par le responsable du traitement, en particulier le moteur de recherche, doit, pour être effectif, l'être de façon totale, sur toutes les extensions du nom de domaine du moteur. Dans le cas contraire, il suffit pour un internaute d'utiliser l'extension « .com » et les extensions non européennes pour retrouver le résultat effacé. De plus, actuellement, le message de Google, qui indique qu'il est possible que des contenus soient déréférencés, incite l'internaute à approfondir sa recherche. Or, c'est aujourd'hui le bras de force qui oppose les moteurs de recherche et la CNIL et qui n'a pas encore été tranché par les juridictions françaises et européennes. Ainsi, la CNIL, saisie par des internautes du refus de déréférencement de liens Internet sur le moteur de recherche Google Search, a demandé à la société Google de procéder au déréférencement de plusieurs résultats et que ce déréférencement soit réalisé sur l'ensemble du moteur de recherche, quelle que soit l'extension géographique du nom de domaine de celui-ci (« .fr », « .com », etc.). Google a fait droit à certaines de ces demandes, mais n'a procédé au déréférencement que sur les extensions géographiques européennes du moteur de recherche. Après mise en demeure et absence de mise en conformité de Google dans le délai imparti, une sanction de 100 000 euros a été prononcée à l'encontre de Google par la CNIL[24]. Comme le résume parfaitement Isabelle Falque-Pierrotin dans une tribune dans le journal *Le Monde* du 29 décembre 2016 :

> […] La position de la CNIL est simple : à partir du moment où Google est installé en Europe et soumis au droit européen et qu'il se présente comme y offrant un service global, le résultat déréférencé doit l'être sur l'ensemble du

[24] Décision de la CNIL, 10 mars 2016. https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu

> moteur. À l'inverse, Google propose qu'un tel déréférencement global n'intervienne que si la recherche s'effectue à partir de la France. En d'autres termes, votre visibilité est effectivement modifiée mais seulement pour vos proches ou pour ceux qui habitent dans votre « territoire réputationnel » attendu ; en revanche, le contenu reste référencé si la recherche s'effectue à partir d'un territoire non français. Cela n'a pas de sens ! Le droit au déréférencement n'est pas un droit « à ne pas voir » localement que Google traite vos données ; c'est un droit à ce que Google ne traite pas certaines de vos données. Retenir l'hypothèse inverse reviendrait à vider les droits des européens de leur substance et à considérer que la portée d'un droit fondamental est à géométrie variable, dépendant non de celui qui l'exerce mais de celui qui en regarde les résultats. […] C'est une question basique de souveraineté, c'est-à-dire d'effectivité de la protection des droits. Ce droit au déréférencement n'est d'ailleurs ouvert qu'au bénéfice des seuls résidents européens ; il ne concerne pas un Chinois en Chine ou un Américain au Nevada. (Falque-Pierrotin, 2016)

Plus encore, le droit à l'oubli numérique peut être dévoyé par le transfert des données personnelles notamment vers les États-Unis. Les transferts de données personnelles sont une réalité dans le contexte de l'économie numérique mondiale actuelle. Aussi, l'Union européenne et les États-Unis ont conclu un accord, le *Privacy shield*, en vigueur depuis le 1er août 2016, pour règlementer le transfert des données personnelles[25] par une entité européenne vers des entreprises établies aux États-Unis, à condition que les entreprises destinataires des données se soient préalablement inscrites sur le registre tenu par l'administration américaine. Les entreprises américaines doivent respecter les obligations et les garanties de fond prévues par le *Privacy shield*. Ce bouclier de protection des données doit conserver les données personnelles uniquement pendant le temps nécessaire à leur traitement. Il est possible de les conserver plus longtemps tout en respectant les principes de protection de la vie privée dans certains cas (notamment l'archivage, l'intérêt public, la recherche scientifique et historique).

Le transfert de responsabilité des États aux acteurs économiques

Le second élément qui fragilise l'efficacité du droit est le report sur les acteurs économiques privés de la mise en œuvre des droits. Ce transfert de

---

25 Cela concerne tout type de données à caractère personnel transférées par une entité depuis l'Union européenne aux États-Unis, notamment des données commerciales, de santé ou de ressources humaines à condition que la société destinataire aux États-Unis ait adhéré au dispositif du *Privacy shield* (COMMISSION EUROPÉENNE, 2016).

responsabilité pallie aux carences de moyens des États et impose indirectement aux agents économiques de réguler leurs pratiques.

Cette tendance actuelle du droit se retrouve en matière de droit à l'oubli numérique. Comme le souligne le rapport annuel de la CNIL de 2016 (CNIL, 2017a), la suppression des données personnelles diffusées sur Internet est compliquée. Les obstacles sont nombreux : absence de réponse de l'organisme ou de la personne qui a diffusé l'information ; absence de formulaire en ligne pour permettre à l'internaute d'exercer son droit ; refus de l'organisme de déréférencer sans forcément justifier sa décision, etc. En effet, en matière de déréférencement, c'est le moteur de recherche qui juge du bien-fondé de la demande qui lui est adressée. Aussi, pour obtenir le droit à l'oubli numérique, l'internaute adresse sa demande au moteur de recherche, généralement *via* un formulaire en ligne. Ce dernier l'examine et décide d'y faire droit ou non. En cas de refus, la CNIL peut intervenir. En conséquence, le moteur de recherche est juge et partie, et le risque, comme le souligne Judith Rochfeld, est « d'assister à une privatisation du jugement de l'information pertinente » (Rochfeld, 2015 : 103).

L'expansion de la soft law

La troisième tendance qui traverse le droit est le développement de la *soft law* et de procédés d'autorégulation. Le droit à l'oubli numérique en est une illustration.

Des codes de bonnes pratiques ont fleuri avant la consécration jurisprudentielle européenne du droit à l'oubli ou avant les dispositions légales qui s'y réfèrent expressément.

Ainsi, la Charte sur la publicité ciblée et la protection des internautes, signée le 30 septembre 2010 par dix associations professionnelles, renforce la protection de la vie privée et le droit des internautes quant à la publicité ciblée. Les associations professionnelles signataires ont défini un ensemble de bonnes pratiques pour garantir un juste équilibre entre l'obligation de transparence, le respect de la vie privée et les impératifs économiques de l'Internet. Huit recommandations ont ainsi été élaborées dont l'information des internautes, l'exercice de leurs droits en matière de publicité ciblée, le rapprochement entre les données de navigation et les données personnelles, la protection des mineurs et le droit à l'oubli des *cookies* (les *cookies* utilisés à des fins de publicité comportementale doivent être limités à une

durée proportionnée à celle du cycle d'achat du produit ou service promu par le biais de telles publicités).

La Charte du droit à l'oubli numérique dans les sites collaboratifs et les moteurs de recherche, signée le 10 octobre 2010, concerne la gestion des données intentionnellement publiées par des internautes, et la mise en œuvre pour ces données des droits constituant le droit à l'oubli. Cette charte a été signée par Benchmark Group (Copains d'avant), Microsoft France, Skyrock.com, Pages jaunes, Trombi.com, Viadeo. Toutefois, Google et Facebook ne sont pas signataires de cette charte du droit à l'oubli numérique.

Ces éléments qui limitent l'efficacité du droit à l'oubli numérique posent la question plus globale du recours à des mécanismes non juridiques pour réguler les droits des internautes. Ils reposeraient à la fois sur la responsabilisation des internautes dans l'utilisation d'Internet et sur la responsabilisation des opérateurs dans le traitement et l'exploitation des données personnelles.

Conclusion

Le cyberespace et le *big data* révolutionnent la conception traditionnelle du droit et l'obligent à s'adapter pour répondre aux nouveaux enjeux et aux nouveaux usages du numérique. Le droit cherche à faire du cyberespace une zone de droits et à concilier la protection des individus, partie la plus faible dans le rapport de force, et les impératifs économiques. Le droit à l'oubli numérique en est une illustration et révèle les enjeux, la complexité et les limites d'un tel exercice. De façon plus globale, le numérique réactualise les interrogations entre le droit et son lien avec la technique. Dans un article intitulé « Code is law », Lawrence Lessig (2000) explique que le régulateur du cyberespace, c'est le code source, et c'est ce dernier qu'il faut appréhender pour comprendre comment y développer aujourd'hui des normes juridiques. À l'heure des algorithmes, les régulateurs publics en Europe « doivent être encouragés dans leurs démarches consistant à descendre dans le code informatique des plateformes et moteurs de recherche pour démasquer les algorithmes trompeurs, déloyaux pour les utilisateurs, voire attentatoires à nos libertés » (Iteanu, 2016 : 148). En effet, le nouveau défi du droit est celui des algorithmes. Dans un univers « algorithmé », quelle autonomie et quelle protection des libertés individuelles et des droits de l'Homme ?

Références bibliographiques

ANDERSON Chris, 2009. *Free! Entrez dans l'économie du gratuit*, trad. fr. par M. Le Séac'h, Paris, Pearson-Village mondial.

BOIZARD Maryline (dir.), 2015. *Le Droit à l'oubli*, Rapport final de recherche, avec le soutien du GIP Mission de recherche Droit et Justice [En ligne] (consulté le 29/10/2017) : http://www.gip-recherche-justice.fr/wp-content/uploads/2015/03/RAPPORT-FINAL-Droit-a%CC%80-loubli-20151.pdf

CARDON Dominique, 2010a. « Les réseaux sociaux en ligne et l'espace public », *L'Observatoire*, 37 (2), p. 74-78.

CARDON Dominique, 2010b. *La Démocratie Internet. Promesses et limites*, Paris, Seuil.

CHIGNARD Simon, BENYAYER Louis-David, 2015. *Datanomics. Les nouveaux business models des données*, Limoges, Fyp.

COINTOT Jean-Charles, EYCHENNE Yves, 2014. *La Révolution* Big data. *Les données au cœur de la transformation de l'entreprise*, Paris, Dunod.

COMMISSION EUROPÉENNE, 2016. *EU-US Privacy Shield. Form for Submission of Request to the U.S. Ombudsperson* [En ligne] (consulté le 27/10/2017). URL: http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf

CNIL (COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS), 2017a. *Rapport d'activité 2016*, 37e rapport, Paris, La Documentation française.

—, 2017b. *Présentation du 37e Rapport d'activité 2016 et des enjeux 2017* [En ligne], Conférence de presse (27 mars 2017), p. 1-14 (consulté le 16/03/2018). URL : https://www.cnil.fr/sites/default/files/atoms/files/dossier_de_presse_cnil_bilan_2016_et_enjeux_2017.pdf

CONSEIL D'ÉTAT, THERY Jean-François, FALQUE-PIERROTIN Isabelle,1998. *Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998*, Paris, La Documentation française.

EL BADAWI Lamia, 2016. « Le droit à l'oubli à l'ère du numérique », *La Revue*, 8 (A.-B. Caire & C. Lantero, dir., « Le droit à l'oubli »), p. 12-27.

FALQUE-PIERROTIN Isabelle, 2016. « Pour un droit au déréférencement mondial », *Le Monde*, 29 décembre.

FARCHY Joëlle, MÉADEL Cécile, SIRE Guillaume, 2015. *La Gratuité, à quel prix ? Circulation et échanges de biens culturels sur Internet*, Paris, Mines ParisTech.

FLICHY Patrice, 2001. *L'Imaginaire d'Internet*, Paris, La Découverte.

GEORGES Fanny, 2008. « Les composantes de l'identité dans le web 2.0, une étude sémiotique et statistique. Hypostase de l'immédiateté », *in* F. Millerand, S. Proulx & J. Rueff (dir.), *Web participatif : mutation de la communication*, actes du 76e Congrès de l'Association canadienne francophone pour le savoir (CFAS ; Québec, 6-7 mai 2008), Québec, Presses de l'Université du Québec, p. 12.

ITEANU Olivier 2016. *Quand le digital défie l'État de droit*, Paris, Eyrolles.

LESSIG Lawrence, 2000. « Code is law. On Liberty in Cyberspace », *Harvard Magazine* [En ligne]. Mis en ligne le 01/01/2000 (consulté le 27/10/2017) : https://www.harvardmagazine.com/2000/01/code-is-law-html

LOVELUCK Benjamin, 2016. « Les formes du pouvoir sur Internet », *in* J.-F. Dortier (dir), *La Communication : des relations interpersonnelles aux réseaux sociaux*, Auxerre, Sciences humaines éditions, p. 324-335.

MERZEAU Louise, 2009. « Du signe à la trace : l'information sur mesure », *Hermès, La Revue*, 53, p. 21-29.

MOURON Philippe, 2012. « L'identité des personnes sur les réseaux : de la richesse de la personnalité à la propriété d'une richesse », *in* S. Agostinelli, D. Augey & F. Laurie (dir.), *La Richesse des réseaux numériques*, actes du colloque Médias 011 (Aix-en-Provence, 8-9 décembre 2011), Aix-en-Provence, Presses universitaires d'Aix-Marseille, p. 215-227.

QUILLET Étienne, 2011. *Le Droit à l'oubli numérique sur les réseaux sociaux*, Mémoire de Master, sous la dir. d'E. Decaux, Paris, Université Panthéon-Assas.

ROCHET Jean-Charles, TIROLE Jean, 2003. « Platform competition in two-sided markets », *Journal of the European Economic Association*, 1 (4), p. 990-1029.

ROCHFELD Judith, 2015. « Les géants d'Internet et l'appropriation des données personnelles : plaidoyer contre la reconnaissance de leur « propriété », *in* M. Behar-Touchais (dir.), *L'Effectivité du droit face à la puissance des géants de l'Internet*, vol. 1, Paris, IRJS Éditions (Bibliothèque de l'Institut de recherche juridique de la Sorbonne – André Tunc 63), p. 89 -104.

WALCZAK Nathalie, 2012. « Repenser le droit à l'oubli », *in* S. Agostinelli, D. Augey & F. Laurie (dir.), *La Richesse des réseaux numériques*, actes du colloque Médias 011 (Aix-en-Provence, 8-9 décembre 2011), Aix-en-Provence, Presses universitaires d'Aix-Marseille, p. 117-128.

Documentation juridique

Textes législatifs et règlementaires français et européens

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « loi informatique et liberté ».

Loi n° 2004-545 du 21 juin 2004 pour la confiance dans l'économie numérique.

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, et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

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.

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.

Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données dit règlement général sur la protection des données (RGPD).

Jurisprudence française

Conseil constitutionnel, décision n° 99-416, 23 juillet 1999.

Conseil constitutionnel, décision n° 2009-580, 10 juin 2009.

Cour de cassation, 1re chambre civile, 12 mai 2016.

Cour de cassation, 1re chambre civile, 3 novembre 2016.

Tribunal de grande instance de Paris, 6 novembre 2013, Max Mosley c. Société Google Inc et Google France.

Tribunal de grande instance de Paris, ordonnance de référé du 19 décembre 2014.

Tribunal de grande instance de Paris, ordonnance de référé du 13 mai 2016.

Décision de la CNIL, 10 mars 2016. https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu

Jurisprudence européenne

CEDH, 17 décembre 2009, n° 16428/05, *Gardel c. France*.

CEDH, 18 décembre 2012, n° 3111/10, *Ahmet Yildirim c. Turquie*.

CJUE, grande chambre, 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, Affaire C-131/12.