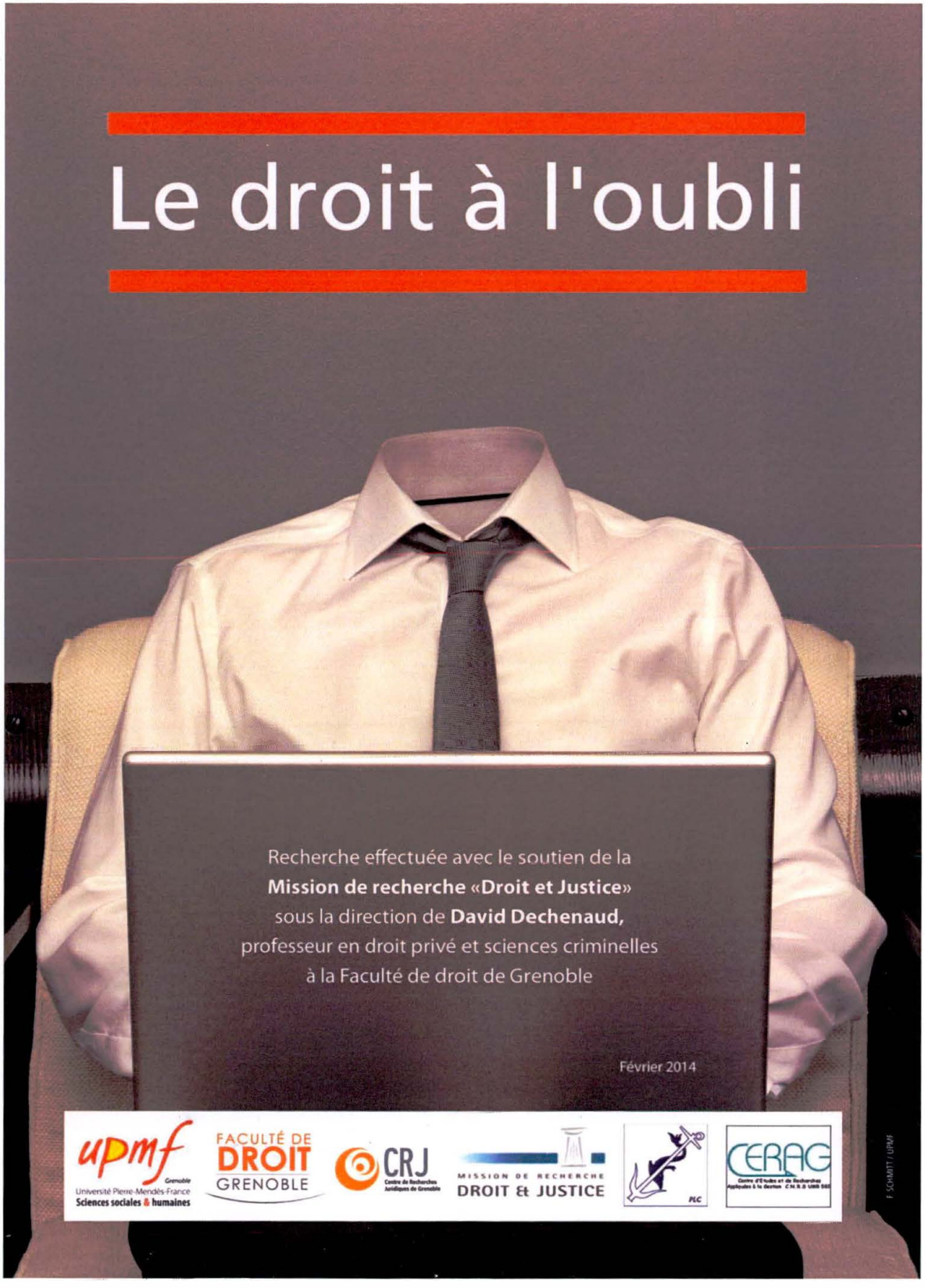
Le droit à l'oubli



Recherche effectuée avec le soutien de la
Mission de recherche «Droit et Justice»
sous la direction de **David Dechenaud,**
professeur en droit privé et sciences criminelles
à la Faculté de droit de Grenoble

Février 2014

upmf Grenoble Université Pierre-Mendès-France Sciences sociales & humaines

FACULTÉ DE DROIT GRENOBLE

CRJ Centre de Recherches Juridiques de Grenoble

MISSION DE RECHERCHE DROIT & JUSTICE

PLC

CERAG

F. SCHMITT / UPMF

Le présent document constitue le rapport scientifique d'une recherche réalisée avec le soutien du GIP Mission de Recherche Droit et Justice (Convention N°212-02.02.26).

Auteurs

Julie Arroyo, *attachée temporaire d'enseignement et de recherche à la Faculté de droit de Grenoble, Université Grenoble Alpes, Centre de recherches juridiques (CRJ).*

Jean-Michel Bruguière, *professeur de droit privé et de sciences criminelles, Faculté de droit de Grenoble, Université Grenoble Alpes, Centre de recherches juridiques, directeur du Centre universitaire d'enseignement en propriété intellectuelle (CUERPI).*

Marie-Laurence Caron-Fasan, *professeur en sciences de gestion, Institut d'administration des entreprises de Grenoble, Université Grenoble Alpes, Centre d'études et de recherches appliquées à la gestion.*

Hafida Belrhali-Bernard, *professeure de droit public à la Faculté de droit de Grenoble, Université Grenoble Alpes, Centre de recherches juridiques (CRJ).*

Latifa Chelbi, *attachée temporaire d'enseignement et de recherche à la Faculté de droit de Grenoble, Université Grenoble Alpes, Centre de recherches juridiques, Centre universitaire d'enseignement en propriété intellectuelle (CUERPI).*

David Dechenaud, *professeur de droit privé et sciences criminelles à la Faculté de droit de Grenoble, Université Grenoble Alpes, Centre de recherches juridiques (CRJ).*

Aurélien Faravelon, *attaché temporaire d'enseignement et de recherche, Université Grenoble Alpes, Centre de recherches Philosophie, langage et cognition et laboratoire informatique de Grenoble.*

Amélie Favreau, *maître de conférences en droit privé et sciences criminelles à l'Institut universitaire de technologie de Grenoble, Centre de recherches juridiques, Centre universitaire d'enseignement en propriété intellectuelle (CUERPI).*

Fabien Girard, *maître de conférences en droit privé et sciences criminelles à la Faculté de droit de Grenoble, Université Grenoble Alpes, Centre de recherches juridiques (CRJ)*

Sophie Guicherd, *docteur en droit privé et sciences criminelles, Faculté de droit de Grenoble, Université Grenoble Alpes, Centre de recherches juridiques (CRJ).*

Nicolas Lesca, *professeur en sciences de gestion, Université Lyon 1, Centre d'études et de recherches appliquées à la gestion.*

Artémi Rallo, *directeur honoraire de l'Agence espagnole de protection des données personnelles.*

Bruno Rasle, *délégué général de l'Association française des correspondants à la protection des données à caractère personnel.*

Cécile de Terwangne, *professeur à la Faculté de droit de Namur, Centre de recherche interdisciplinaire en information, droit et société(CRIDS).*

François Viangalli, *maître de conférences en droit privé et sciences criminelles à la Faculté de droit de Grenoble, Université Grenoble Alpes, Centre d'études sur la sécurité internationale et les coopérations européennes. (CESICE)*

SOMMAIRE

(Une table des matières détaillée figure à la fin de l'ouvrage)

Introduction[1]

La présente recherche est une réponse faite à un appel à projet lancé par le GIP « droit et justice » en 2011. La Mission souhaitait que soit réalisée une étude portant sur une notion mal définie, et non consacrée par le droit positif. L'appel faisait état de la difficulté à donner un contenu normatif au « droit à l'oubli », compte tenu de la subjectivité du concept même d'oubli. C'est donc par référence à d'autres principes définis par le droit français que le « droit à l'oubli » renvoi, et en particulier au droit au respect de la vie privée. L'appel à projet en déduisait que le « droit à l'oubli » est « une notion non juridique recouvrant plusieurs droits juridiquement (plus ou moins) protégés ». Dans un contexte alors marqué par les projets de refonte de la directive européenne 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, la Mission de recherche proposait de s'intéresser à plusieurs questions:

- le droit à l'oubli doit-il constituer un droit autonome et fondamental?
- le droit à l'oubli doit-il être une simple déclinaison du droit à la protection de la vie privée ?
- quel serait le contenu du droit à l'oubli?
- quelles seraient ses limites?
- quelles seraient ses incidences juridiques?

La réponse apportée à cet appel à projet fait l'objet de cet ouvrage. L'équipe a fait le choix de proposer une approche large de la question, sans la limiter aux seules questions relatives à la protection des données personnelles. La présentation de la problématique et objectifs de la recherche (I) précédera l'explication des choix méthodologiques et du terrain de la recherche (II), puis quelques éléments de conclusion (III). Cette recherche étant loin d'épuiser le sujet, des pistes de recherches et quelques perspectives seront ensuite présentées (IV).

I- Problématique et objectifs de la recherche

L'étude du droit à l'oubli conduit à s'interroger sur la manière dont l'oubli est saisi par le droit. Au moment où un projet de règlement européen « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnelles et à la libre circulation de ces données » est au centre de toutes les préoccupations, il aurait été possible d'orienter l'ensemble de la réflexion sur le droit à l'oubli numérique. Le choix a précisément été celui de ne pas avoir une approche aussi limitée du sujet. En effet, la problématique du droit à l'oubli numérique peut difficilement être détachée de considérations qui dépassent la seule question de l'informatique et de l'Internet (droit au respect de la vie privée, liberté d'expression et droit à l'information, etc.). En outre, le droit à l'oubli n'étant pas en lui-même consacré par le droit sous cette dénomination, l'étudier ne pouvait pas se concevoir sans le replacer dans un environnement

[1] David Dechenaud, Professeur de droit privé et sciences criminelles à la Faculté de droit de Grenoble, Université Grenoble Alpes, Centre de recherches juridiques (CRJ)

juridique plus large. La **problématique** retenue était donc celle de déterminer les fondements du droit à l'oubli, ses manifestations en droit positif et d'engager une réflexion sur le droit prospectif (v. réponse à l'appel à projet).

Les travaux menés ont rapidement permis de se convaincre que la question du droit à l'oubli dans le champ du numérique présente une nette spécificité. Cependant, une approche plus large de la question, faisant notamment appel aux expériences étrangères, montre qu'une étude ne portant que sur le droit à l'oubli numérique aurait été parcellaire pour ne pas dire étriquée. Les **objectifs des travaux** étaient donc triples.

S'agissant du cas particulier du *droit à l'oubli numérique*, la recherche présente l'historique du projet de règlement européen et du concept de « droit à l'oubli » qui s'avère être essentiellement destiné à fournir une visibilité politique contemporaine à une question déjà ancienne. Cela n'a pas empêché le déferlement des groupes de pression qui ont fait feu de tout bois envers ce projet de texte qui se trouve, dans son dernier état, assez largement privé de sa substance quant au « droit à l'oubli ». Le rapport s'est donné pour objectif, sur ce point, de mettre en lumière les véritables enjeux juridiques de ce projet de règlement.

La recherche a également pour but d'aborder la question de *l'oubli au-delà du seul univers numérique et au-delà de son appréhension juridique*. La possibilité, pour un sujet de droit, de voir un certain nombre d'informations le concernant être effacées, a été étudiée à la fois dans le domaine du droit informatique et liberté en vigueur, du droit administratif, et des droits de la personnalité. À ce sujet, le but était de faire ressortir la place que le droit concède aux revendications qui tendent à obtenir l'oubli de certaines informations, dans une société aussi préoccupée par le devoir de mémoire. La recherche aborde également la question au prisme des sciences de gestion et de l'informatique : elle est donc pluridisciplinaire.

Enfin, la recherche aborde aussi la problématique de l'oubli *au-delà du droit français*. La considération qu'une société accorde à la question de l'oubli dépend sans aucun doute de *l'environnement culturel considéré*, ce que l'étude du droit des États-Unis d'Amérique, du droit anglais et du droit espagnol avait pour objectif de démontrer.

II- Choix méthodologiques et terrains de recherche

Afin d'atteindre ces trois objectifs, le choix méthodologique effectué a été celui d'une approche résolument pluridisciplinaire. Le terrain de recherche n'est donc pas limité à la seule règle de droit. Ce choix de retenir plusieurs terrains de recherche a orienté de manière décisive la façon dont le rapport est présenté : le travail est véritablement collectif, ce qui conduit à mettre en avant des regards croisés sur une thématique unique.

A-Terrain de recherche : approche pluridisciplinaire, approche collective

Le choix de ne pas se cantonner à l'unique étude de la règle de droit français générale et abstraite a orienté l'ensemble de la recherche effectuée, et en explique à la fois la richesse et les faiblesses. La richesse se manifeste précisément au moment de présenter le terrain de la recherche. La problématique et les objectifs des travaux menés permettent d'appréhender la question du droit à l'oubli de manière globale, en donnant une réponse qui se veut complète : la recherche porte à la fois sur le droit privé, le droit public, l'informatique, la gestion des systèmes d'information. Elle aborde la question au prisme du droit national, mais aussi européen, et étudie

l'exemple de trois droits étrangers (États-Unis d'Amérique, Angleterre, Espagne). Les terrains de recherche varient selon le champ disciplinaire dans lequel s'inscrivent les travaux qui ont été réalisés.

B-Choix méthodologiques : approche collective, regards croisés

Cette richesse quant aux terrains de recherche retenus est à l'origine d'une faiblesse quant à la méthode de travail et, en conséquence, à la présentation du rapport. En effet, les différents terrains de recherche ont été abordés par des chercheurs aux compétences différentes, examinant la problématique au prisme de leur discipline d'appartenance. Le rapport présente donc, successivement, les différents aspects de la question. Cette construction du rapport n'est pas, contrairement à ce que l'on pourrait penser, une solution de facilité. Elle est apparue inévitable en ce qu'il est impossible de prétendre fusionner, dans un ensemble unique, des questions aussi diverses que celle de l'oubli dans le domaine des archives publiques ou celle du rôle du délégué à la protection des données personnelles. Telle est la conséquence de la pluridisciplinarité qu'on dit souvent être peu familière aux chercheurs juristes : accepter de dérouler la thématique abordée sous ses différents angles, sans chercher à présenter, d'une manière qui se révélerait nécessairement très artificielle, ces approches comme n'en faisant qu'une. L'oubli est probablement protéiforme, et la revendication d'un droit à l'oubli aussi.

III- Conclusions de la recherche : l'émergence d'un « droit à l'oubli », entre utopie et réalité

À l'issue de ce travail de recherche, plusieurs conclusions se dégagent. Elles ne peuvent être présentées ici de manière exhaustive, précisément car la méthode de travail choisie consistait à faire une étude dans plusieurs champs disciplinaires différents (v. *supra*). En conséquence, il est impossible de parvenir à dresser une synthèse unique, qui serait nécessairement réductrice. Elle se présenterait comme une juxtaposition de plusieurs conclusions, sans parvenir à donner une image fidèle du résultat des travaux conduits par les différents chercheurs dans leurs domaines respectifs de travail. Ainsi, l'ouvrage se présente en une succession de contributions présentant l'état du droit et des réflexions dans chaque discipline. Telle est la richesse d'une recherche collective en droit : permettre au lecteur de confronter les points de vue et les analyse sans prétendre les compiler, de manière nécessairement réductrice, en une conclusion globale. Assurément, l'exercice serait plus simple si, comme en sciences du vivant, il suffisait de se prononcer objectivement sur l'efficacité d'un médicament après plusieurs années d'observation clinique !

Malgré cela, il est bien sûr possible de retirer de cette recherche un certain nombre de conclusions et de pistes de travail, répondant en cela aux questionnements soulevés par l'appel à projet (v. introduction).

- En premier lieu, le « **droit à l'oubli** » est un **concept dont l'existence ne paraît pas indispensable** pour assurer la protection des personnes en matière de traitements de données à caractère personnel.

- En deuxième lieu, **l'effectivité des dispositifs** existants qui tendent à la protection de l'oubli devrait être une **préoccupation majeure** des autorités nationales et européennes.

- En troisième lieu, la recherche de l'oubli se heurte et se heurtera toujours à des **intérêts opposés** avec lesquels il convient de l'**équilibrer**.

A-Le droit à l'oubli, un concept à l'utilité non avérée

Le droit à l'oubli relève davantage du slogan législatif que d'une notion juridique précisément définie. Le rapport montre que le **droit au respect de la vie privée**, dont les contours méritent d'être renouvelés, serait pleinement satisfaisant pour parvenir à la protection envisagée. Procéder différemment aurait pour effet d'isoler artificiellement la question dite du « droit à l'oubli » de celle de la protection des droits de la personnalité. La recherche propose de clarifier, pour l'avenir, les rapports qu'entretiennent les dispositions de la loi « informatique et libertés » et les dispositions du Code civil. L'articulation entre ces dernières dispositions, qui constituent le droit commun, et la loi de 1978, qui n'est rien moins que l'application du droit commun à une matière particulière, ne sont plus satisfaisants en ce début de XXI^{e} siècle. L'étude du droit anglais permet également de s'en convaincre, compte tenu de l'approche qui est faite outre-Manche du droit à l'oubli au travers du concept de « *privacy* ».

Concernant la législation spécifique, dans le domaine de la protection des données personnelles, le rapport propose de consacrer le **droit à l'autodétermination informationnelle** plutôt que de formaliser un droit à l'oubli. Le droit à l'autodétermination informationnelle, bien connu des juristes allemands, est un véritable concept juridique à la différence du « droit à » l'oubli qui n'en est pas un. Le droit ne saurait garantir l'oubli, qui ne se décrète pas. En revanche, il est en mesure d'accorder au sujet de droit des prérogatives qui lui permettent d'obtenir l'effacement ou l'anonymisation de données personnelles qui le concernent, ce qui rend l'oubli possible. C'est donc autour de ce droit à l'autodétermination informationnel que mérite d'être repensé l'arsenal législatif français. Cet arsenal, aujourd'hui essentiellement contenu dans la loi « informatique et libertés », est déjà très complet : il est apparu à l'équipe de recherche et aux praticiens du droit qu'elle a rencontrés qu'il conviendrait avant tout d'assurer l'effectivité du droit en vigueur avant de penser à créer de nouvelles garanties dont l'applicabilité est tout sauf... garantie.

B-L'effectivité des dispositifs tendant à la protection de l'oubli

Il s'agit de la seconde préoccupation qui ressort du rapport. D'une manière générale, cette effectivité de l'oubli, qu'il se traduise par un droit à l'autodétermination informationnelle, par le droit au respect de la vie privée ou par des dispositions spécifiques propres à certains domaines (archives publiques), est une difficulté majeure qui ne trouve pas de solution satisfaisante en se cantonnant au niveau national ou européen.

Sur le plan national et européen, le rôle des différents acteurs qui veillent à la mise en oeuvre des règles existantes est mis en lumière. Le Correspondant informatique et liberté (ou délégué à la protection des données personnelles) est l'une des pierres angulaires du dispositif s'agissant de l'autodétermination informationnelle dans le champ informatique. Le recours à des instruments préventifs, comme les chartes dites « de bonnes pratiques », semble également être un élément non négligeable alors que l'application effective de la règle de droit est loin d'être avérée. Par ailleurs, le coût de l'effacement ou de l'anonymisation des données étant plus important que celui de leur conservation, une analyse économique de la question juridique paraît difficilement contournable. La conception technique des systèmes d'information doit être faite, en amont, en tenant compte de l'obligation de pouvoir ensuite assurer la traçabilité et la suppression des données qu'ils contiennent. La recherche n'a pas permis d'identifier l'existence

d'instruments de « *soft law* » suffisants en la matière, et le rapport invite donc les acteurs des secteurs professionnels concernés à y remédier.

Sur le plan international, les questions de droit international privé, le pragmatisme dont il convient de faire preuve sur le plan technologique et l'expérience déjà très nuancée de l'application réelle, en droit positif, des dispositions de la loi « informatique et libertés » sont abordés dans le rapport. La question de l'oubli ne se pose qu'au sujet d'informations préalablement rendues publiques. Or, le développement des technologies de communication, notamment numériques, conduit à une dispersion sans cesse plus importante des lieux de stockage des données concernées. L'effectivité du droit en la matière suppose une approche mondialisée. C'est alors que resurgit l'importance décisive du système juridique dans lequel s'intègre la règle de droit considérée : à la lecture du rapport, le lecteur se convaincra qu'il est difficile d'imaginer rapprocher les conceptions européenne et américaine de la question, à court ou moyen terme. L'étude du droit des États-Unis d'Amérique prouve que les perspectives d'évolution y restent très limitées, si bien que les différences d'approches entre les deux continents paraissent avoir vocation à perdurer. Une telle conclusion semble bien pessimiste. Elle incite surtout les États à accepter l'idée que, sur ce sujet comme sur bien d'autres, il n'est désormais plus possible d'avoir une approche isolationniste, sous peine d'élaborer des législations non efficientes et donc, au final, de perdre son temps à construire des textes qui ne produiront pas les effets escomptés.

C- L'oubli, la mémoire et le droit

La revendication sociale d'une possibilité de voir certaines informations personnelles être oubliées, aussi légitime soit-elle, se heurte inévitablement à d'autres intérêts avec lesquels il convient de la concilier. Le rapport le démontre à la fois sur le plan philosophique et juridique. L'approche philosophique révèle toute l'ambiguïté des rapports qu'entretiennent le désir d'oubli et le souhait de mémoire dans la société. On ne s'étonnera alors pas de trouver, dans le rapport, des manifestations juridiques du « droit à » l'oubli et du « devoir » de mémoire.

Cette recherche d'équilibre est juridiquement délicate et constitue le point d'achoppement le plus important entre la tradition française, d'une part, et celles d'autres États dont les États-unis d'Amérique, d'autre part. Liberté d'expression *versus* droit au respect de la vie privée ou droit à l'autodétermination informationnelle : la confrontation semble universelle, mais la détermination du point d'équilibre ne l'est pas. Il n'est d'ailleurs pas certain que l'approche régionale permette de lever toutes les difficultés. Ainsi, le projet de règlement européen paraissait vouloir privilégier le droit à la protection de la vie privée en consacrant le droit à l'oubli, tandis que le droit du Conseil de l'Europe apporte une protection particulièrement élevée à la liberté d'expression.

Ainsi, beaucoup d'**intérêts publics sont** en cause : il faut aussi composer avec la nécessaire conservation des archives, ou les exigences d'ordre public qui conduisent à la création de fichiers policiers et judiciaires, par exemple. Il existe, par ailleurs, un certain nombre d'**intérêts privés** qui ne peuvent pas, non plus, être ignorés : la continuité des activités économiques, la nécessité de préconstituer des preuves en matière civile et commerciale notamment, etc. La distinction entre ces intérêts publics et privés ne révèle pas une opposition : on pense, en particulier, à la liberté du commerce et de l'industrie ayant mené le développement d'activités économiques faisant de la gestion de ces données l'objet même de leur commerce.

IV- Pistes de recherche et perspectives

À l'issue de ces réflexions croisées, plusieurs pistes de réflexions (non exhaustives) peuvent être proposées, en lien avec chacune des trois conclusions précédemment présentées.

A- Le droit à l'oubli, un concept à l'utilité non avérée

- **Repenser l'articulation** des articles du **Code civil** se rapportant à la protection de la vie privée, les **dispositions de la loi « informatique et libertés »** relatives aux données personnelles et les **autres textes** garantissant des possibilités d'effacement de telles données.
- **Reconnaître le droit à l'autodétermination informationnelle**, réunissant de nombreuses prérogatives actuellement prévues par la loi de 1978 en faveur des personnes dont les données personnelles font l'objet d'un traitement informatique.
- S'interroger sur les moyens de protéger l'oubli qui serait revendiqué par des **personnes morales**.

B- L'effectivité des dispositifs tendant à la protection de l'oubli

- Renforcer le rôle des Correspondants informatique et libertés (Délégués à la protection des données personnelles) et, plus généralement, **améliorer l'effectivité du dispositif existant** en droit positif avant d'envisager son extension.
- **Favoriser le recours à des instruments** de « *soft law* » (chartes de bonnes pratiques, principes déontologiques), pour les acteurs du numérique et au-delà d'eux (médias, par exemple).
- Engager une réflexion relative au droit de la protection des données personnelles **au-delà du seul cadre de l'Union européenne**.

C- L'oubli, la mémoire et le droit

- Prévoir, par un texte spécifique, l'interdiction de faire mention de faits relevant du **passé judiciaire d'un individu**, ou *a minima* exiger leur anonymisation.
- Contraindre les entreprises de presse à **contextualiser les informations** qu'elles diffusent, y compris rétroactivement pour la presse en ligne en mettant à jour des articles antérieurs.
- **Recourir** de manière plus massive à l'**anonymat** ou au **pseudonymat**, qu'il s'agisse d'une obligation imposée aux gestionnaires de systèmes d'information ou d'une incitation adressée aux sujets de droit (notamment les internautes).
- Engager une réflexion au sujet de la **désindexation**

PREMIERE PARTIE :

« L'oubli, le Droit, les droits »

CHAPITRE 1 :

Droit à l'oubli ou droit à l'autodétermination informationnelle ?[1]

Introduction

1. Le droit à l'oubli est aujourd'hui au coeur d'intenses débats. Depuis des mois déjà, le législateur de l'Union européenne s'interroge sur l'impérieuse nécessité d'un tel droit dans l'environnement digital. Le Conseil de l'Europe a quant à lui exprimé sa préoccupation sur le sujet, certains hommes politiques nationaux ont également fait entendre leur voix tandis que des autorités de protection des données personnelles, des organismes oeuvrant dans le domaine des droits de l'homme, des académiques et des experts se sont joints à la procession, en provenance de différents horizons géographiques.

Ce qui est en jeu c'est le droit pour les individus de voir effacer des informations les concernant après un certain laps de temps.

Cela a déjà été, dans une certaine mesure, reconnu comme un droit sous deux angles différents : à l'égard du passé judiciaire et en tant qu'élément du régime de protection des données à caractère personnel[2]. Mais le développement des technologies de l'information et de la communication (TIC) a irrémédiablement entraîné la nécessité de repenser l'étendue du champ de ce droit. Le progrès technologique a un impact considérable en cette matière. Internet a induit le besoin d'établir de nouveaux équilibres entre la libre communication de l'information et l'autodétermination individuelle. Cet équilibre est précisément ce qui est en jeu aujourd'hui dans le droit à l'oubli.

Section 1 - Définition et contexte du droit à l'oubli

I - Que faut-il entendre par « droit à l'oubli » ?

2. Il est impératif de comprendre correctement ce qui est réellement entendu par droit à l'oubli avant d'en étudier le régime juridique. L'idée n'est pas de permettre à quelqu'un de réécrire le passé et d'effacer les traces (déplaisantes) de son passage sur terre.[3] L'idée est de veiller à ce que

---

1 par Cécile de Terwangne, Professeur faculté de Namur, Centre de Recherche, Information, Droit et Société CRIDS Belgique

2 Voy.infra, Section4/Iet II.

3 Lors de l'"Innovation Conference Digital, Life, Design' à Munich le 22 janvier 2012, Viviane Reding, Vice-Présidente de la Commission européenne et Commissaire à la Justice de l'UE, annonça l'insertion d'un droit à l'oubli dans la réforme de la protection des données. Elle affirma: "It is clear that the right to be forgotten cannot amount

le présent d'un individu ne soit pas encombré par son passé. Le passé est le passé ; il ne devrait pas remonter à la surface de manière récurrente. Le changement et l'évolution font partie de la nature humaine. Les individus ne devraient pas être réduits à leur passé. Le droit à l'oubli ne signifie pas l'effacement de l'information. Il doit plutôt s'entendre de ce qu'on doit à un moment arrêter de faire remonter à la surface des données du passé. C'est la première signification du droit à l'oubli. Dans cette acception, ce droit est conditionné par l'écoulement du temps et se rapporte à des informations (re)rendues accessibles au public.

Mais un autre sens est donné aujourd'hui à cette notion. L'expression « droit à l'oubli » est utilisée, à tout le moins dans le cadre des institutions européennes, ainsi qu'on le verra dans la suite de cette étude, pour couvrir une réalité plus vaste que le lien entre passé et présent. Dans sa communication précédant le processus de révision de la directive 95/46 relative à la protection des données à caractère personnel, la Commission européenne évoque le droit à l'oubli comme étant « le 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. »[4] Le droit à l'oubli, en ce sens, est lié à la finalité du traitement des données et à l'expiration de l'utilité des données au regard de cette finalité. Cela étant, la volonté de la personne concernée par les données peut également être le facteur déclencheur de ce droit à l'oubli aux contours nouveaux.

La proposition de règlement général de protection des données[5] publiée en janvier 2012 par la Commission européenne dans le but de remplacer la directive 95/46[6] accentue davantage le rôle déterminant de la volonté de l'individu en ce qui concerne le droit à l'oubli.

Cette évolution reconnait le droit à l'oubli comme un élément de l'auto-détermination informationnelle (voy. les développements au point 2 ci-dessous). Dans ce sens, ce droit n'est plus conditionné par l'écoulement du temps et ne concerne pas nécessairement une information (re)mise à disposition du public. Il s'agit plutôt du droit d'obtenir de quelqu'un qu'il oublie (supprime) ce qu'il savait car il n'est plus légitime de continuer à détenir cette information. Nous verrons que cette présentation du droit à l'oubli par la Commission européenne est simpliste.

---

to a right of the total erasure of history. » (V. Reding, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age", consultable à : http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF)

4 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», 4 novembre 2010, COM(2010) 609 final, p. 9. De même, « Si un individu ne veut plus que ses données soient traitées ou enregistrées par un responsable de traitement, et s'il n'y a pas de raison légitime de les conserver, les données devraient être retirées du système » (notre traduction : "If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system.", V. Reding, op. cit.)

5 Commission européenne, Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), COM(2012) 11 / 4, 25 janvier 2012.

6 Directive 95/46/CE du Parlement et du Conseil 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, J.O.C.E., n° L 281 du 23 novembre 1995, pp. 31– 50.

Dans différents cas, ce droit n'impliquera pas d' « arrêter de savoir » mais plutôt d'arrêter de diffuser les données ou d'arrêter de les indexer sur le web.

II- Le contexte spécifique d'internet

L' « eternity effect » ou effet d'éternité

3. L'infaillibilité de la "mémoire totale" d'Internet contraste avec les limites de la mémoire humaine.[7] Or la mémoire peut être celle de la rancune, de la vengeance et du dénigrement[8]. Grâce à son « eternity effect »[9], son effet d'éternité, Internet préserve les souvenirs bons et mauvais, les erreurs du passé, les écrits, photos ou vidéos qu'on voudrait plus tard ne jamais avoir postés sur le Web. « La transparence des informations sur des erreurs de trajectoires, les condamnations, les modes de vie de certains pourraient affecter et troubler la vie d'autres membres de la parenté. Des rapprochements malheureux ou malhonnêtes deviennent très faciles sur le Net. Ils pourront être utilisés par quiconque veut mettre son prochain en difficulté. »[10] La Commissaire européenne à la Justice Viviane Reding s'est exclamée il y a quelques temps: « Ainsi qu'on le dit: 'Dieu pardonne et oublie, mais le Web jamais !' C'est pourquoi le droit à l'oubli est si important pour moi. Avec de plus en plus de données privées circulant sur le Web – spécialement sur les sites de réseaux sociaux – les gens devraient avoir le droit de faire supprimer complètement leurs données. »[11]

La dé-contextualisation

4. Le « nouveau » droit à l'oubli digital réclamé aujourd'hui et inséré dans la proposition de règlement de la Commission européenne est clairement lié à certaines spécificités d'Internet. L' « effet d'éternité » de la mémoire électronique doit être combiné à l'efficacité des moteurs de recherche pour ramener à la surface du Net la moindre information, retirée de son contexte initial, et rassembler toutes les pièces. Cela débouche sur un portrait recomposé, quoique souvent hétérogène, des individus visés par une requête à partir d'un moteur de recherche. Lié à la « mémoire absolue » d'Internet, un tel portrait peut être constitué de caractéristiques du passé éternellement présentes. Le résultat peut parfois être dommageable d'une façon ou d'une autre pour la personne concernée. Et ce n'est pas seulement l'information diffusée par des tiers qui peut susciter des préoccupations. L'embarras et les soucis peuvent découler ce que l'on a mis soi-même sous les projecteurs du Web. Ce que vous avez accepté de partager avec certains

---

7 I. Székely, "The right to forget, the right to be forgotten. Personal reflections on the fate of personal data in the information society", in S. Gutwirth, R. Leenes, P. De Hert and Y. Poullet (eds.), European data protection: in good health?, Dordrecht, Springer, 2012, pp. 347-363.

8D.Ettighoffer, « Les droits de l'homme numérique : le droit à l'oubli », disponible à l'adresse http://www.ettighoffer.com/fr/idees/idees8.html

9 Walz, S., « Relationship between the freedom of the press and the right to informational privacy in the emerging Information Society », 19e Conférence international des commissaires à la protection des données, Bruxelles, 17-19 septembre 1997, p. 3.

10 D., Ettighoffer, op. cit.

11 Notre traduction. " As somebody once said: "God forgives and forgets but the Web never does!" This is why the "right to be forgotten" is so important for me. With more and more private data floating around the Web – especially on social networking sites – people should have the right to have their data completely removed", V. REDING, "Why the EU needs new personal data protection rules?", The European Data Protection and Privacy Conference,Bruxelles,30novembre2010,
http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700.

destinataires parce qu'ils appartiennent à un cercle déterminé (amis, famille, membres d'un groupe d'intérêt, etc.), vous ne voulez pas nécessairement le rendre accessible à quiconque dans un contexte différent. Toutefois, grâce aux moteurs de recherche, ces informations deviennent accessibles hors du cercle et du contexte initiaux. Il s'avère que l'on peut subir un préjudice du fait d'une information que l'on a spontanément diffusée soi-même à un stade antérieur.[12]

On a en conséquence vu apparaître des entreprises spécialisées dans la gestion de la « e-réputation » des individus et des entités juridiques sur Internet. Ces entreprises proposent de réaliser des opérations de nettoyage soit en « one-shot » soit sur le long terme, en vue de préserver ou de restaurer la réputation et l'image de celui qui fait appel au service.

La nécessité d'une décision d'effacer

5. Une autre spécificité d'Internet est que, contrairement à ce qui se passe dans la vie « physique », effacer dans le monde digital nécessite de prendre une décision. C'est un processus conscient et désiré. Il faut avoir la volonté de supprimer l'information.

Le coût économique de l'effacement

6. En outre, il est devenu moins onéreux de conserver les données que de les détruire ou de les anonymiser. Les capacités de stockage ont en effet crû de manière exponentielle tandis que leur coût a diminué. Dans le même temps, « oublier de nos jours est une affaire coûteuse »[13]. La sélection et l'évaluation des données sont des opérations indispensables avant toute suppression Mais ces opérations sont coûteuses en temps de travail et dès lors coûteuses tout court.[14] L'exercice du droit à l'oubli va dès lors à l'encontre du courant économique naturel.[15]

Par ailleurs, dans le même sens, l'effacement des données à caractère personnel va à l'encontre du modèle économique d'Internet. Une des cibles du droit à l'oubli consiste dans les traces électroniques que les navigateurs du Web laissent inconsciemment derrière eux pendant qu'ils circulent sur le Net. Associées aux cookies, à la conservation des adresses IP, aux analyses de navigation sur Internet, à l'enregistrement des requêtes par les moteurs de recherche, etc., toutes ces données présentent une grande valeur dans une perspective économique. La conservation longue durée de toutes ces traces inconscientes par la plupart des acteurs d'Internet est précieuse pour ces derniers étant donné le modèle économique de l'offre de service sur le Net : la plupart des produits ou services d'information sont apparemment gratuits alors qu'ils sont financés en réalité par de la publicité taillée sur mesure individuellement et par la publicité comportementale. Cela limite assurément l'enthousiasme à effacer de telles informations.

---

12 Sur le risque de dé-contextualisation dans les réseaux sociaux, voy. F. Dumortier. "Facebook and risks of "de-contextualization" of information", 2009, disponible à l'adresse:
http://works.bepress.com/franck_dumortier/1. Sur les sites de réseaux sociaux, il a été démontré que la perte de contrôle de l'utilisateur se note à trois niveaux: la création de données à caractère personnel, leur accessibilité et leur suppression (J.-P. Moiny, 'Cloud based Social Network Sites : under whose Control ?', Investigating cyber law and cyber ethics, 2012, pp. 147-219).

13 Notre traduction: "Nowadays forgetting is a costly affair » (I. Szeleky, op. cit.)

14 Ibidem.

15 Contrôleur européen à la protection des données, avis du 14 janvier 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée - «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», J.O. C 181/01, 22 juin 2011.

Section 2 - L'autonomie informationnelle ou l'auto-détermination informationnelle

I- La notion d'autonomie/auto-détermination informationnelle

7. L'autonomie ou l'auto-détermination informationnelle signifie la possibilité de contrôle de ses propres informations personnelles, c'est-à-dire le droit des individus de déterminer quelles informations les concernant peuvent être communiquées à qui et à quelles fins[16]. Le « contrôle » recouvre également, non pas tant la possibilité de décider de l'utilisation de ses données, mais à tout le moins le droit d'être au courant de leur sort, d'être informé de qui sait quoi sur soi et pour en faire quoi.

L'autonomie informationnelle est dérivée du droit au respect de la vie privée, cette dernière étant entendue dans ce cas non dans son acception classique comme intimité ou secret mais en tenant compte de l'autre dimension qui lui est attachée : l'autonomie individuelle[17], la capacité de faire des choix, de prendre des décisions éclairées, en d'autres termes de garder le contrôle sur certains aspects de sa vie. Mise en relation avec les informations personnelles, cette autonomie individuelle signifie l'autonomie informationnelle ou l' « auto-détermination informationnelle », pour reprendre l'expression énoncée pour la première fois par la Cour constitutionnelle allemande dans sa décision cruciale de 1983[18].

Dans sa « Déclaration sur les moyens de communication de masse et les droits de l'homme » contenue dans la Résolution 428 (1970), l'Assemblée parlementaire du Conseil de l'Europe avait défini en 1970 le droit au respect de la vie privée comme « le droit de mener sa vie comme on

---

16 C. de Terwangne, 'Internet Privacy and the Right to Be Forgotten/Right to Oblivion', Revista de Internet, Derecho y Politica, 2012, p. 112, disponible à l'adresse www.idp.uoc.edu; A. Rouvroy, Y. Poullet, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel: une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie », in Etat de droit et virtualité (K. Benyekhlef, P. Trudel (eds.)), Montréal, Thémis, 2009, pp. 157-222, disponible à l'adresse http://www.crid.be/pdf/public/6050.pdf; H. Burkert, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », Droit de l'Informatique et des Télécoms, 1985, 8-16 ; C. de Terwangne, « Le rapport de la vie privée à l'information », in Droit des technologies de l'information. Regards prospectifs (dir. E. Montero), Cahiers du CRID n° 16 Bruxelles, Bruylant, 1999, p. 144 ; Th. Léonard, Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in F. Rigaux, La vie privée : une liberté parmi les autres ?, Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.; G Hornung, C Schnabel, « Data protection in Germany I: The population census decision and the right to informational self-determination », Computer Law & Security Review, 2009, pp. 84-88; P. Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", The American Journal of Comparative Law,Vol.37, No. 4, 1989, pp. 675-701, disponible à l'adresse :http://scholarship.law.berkeley.edu/facpubs/866.

17 Pour la reconnaissance explicite d'un droit à l'autodétermination ou l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'article 8 CEDH, voy. Cour eur. D.H., Evans c. Royaume-Uni, arrêt du 7 mars 2006, req. n° 6339/05 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007) ; Tysiac c. Pologne, arrêt du 20 mars 2007, req. n° 5410/03 ; Daroczy c. Hongrie, arrêt du 1er juillet 2008, req. n° 44378/05.

18 BundesVerfassungsGericht, 15.12.1983, Volkszählungsurteil, BVerfGE Bd. 65, S. 1 ff: "[...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the [German Constitution]. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest."

l'entend avec un minimum d'ingérence ». Près de trente ans après l'adoption initiale de ce texte, l'Assemblée a précisé dans sa Résolution 1165 (1998) que « Pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition « le droit de contrôler ses propres données »[19].

En Europe, cette auto-détermination informationnelle a été reconnue et protégée comme un droit, le droit à la protection des données à caractère personnel. La Cour européenne des droits de l'homme a fait découler cette nouvelle dimension de la vie privée de l'article 8 de la Convention européenne des droits de l'homme (CEDH).[20] La Convention 108 du Conseil de l'Europe Convention[21] a établi depuis 1981 le droit à la protection à l'égard du traitement automatisé des données à caractère personnel. La Charte des droits fondamentaux de l'Union européenne[22] est le premier catalogue international général de droits et libertés fondamentales à mentionner le droit à la protection des données comme un droit autonome, protégé en tant que tel. Son article 8.1 stipule que « Toute personne a droit à la protection des données à caractère personnel la concernant». Enfin, la directive européenne 95/46 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[23] met en place un régime juridique particulièrement détaillé, actuellement en cours de révision pour l'adapter aux changements radicaux apparus depuis son adoption.

Bien évidemment, ce droit à l'auto-détermination informationnelle n'est pas absolu. Des intérêts publics ou privés prépondérants doivent être pris en considération, découlant sur de possible exceptions ou limites au contrôle individuel sur les données.

Dans l'environnement digital, et en particulier sur Internet, des quantités impressionnantes d'informations se rapportant à des individus sont traitées : elles sont diffusées, communiquées, partagées ; on peut les sélectionner, les télécharger, les enregistrer et en faire toutes sortes d'utilisations. Le contrôle sur les destinataires de l'information est particulièrement délicat.[24] Ainsi que mentionné antérieurement, les moteurs de recherche comme Google rassemblent des informations provenant de contextes variés. En oeuvrant de la sorte, ils sortent les données de leur cercle initial et ont pour effet qu'il est extrêmement difficile de contrôler à qui les données sont communiquées. Une autre difficulté concerne le moment auquel la communication a lieu. Ce

---

19 Résolution 1165(1998) de l'Assemblée parlementaire du Conseil de l'Europe sur le droit au respect de la vie privée, adoptée le 26 juin 1998 (c'est nous qui soulignons).

20 Voy., parmi d'autres, Cour eur. D.H., Rotaru c. Roumanie, 4 mai 2000, req. n° 28341/95, § 43; Amann c. Suisse, 16 février 2000.

21 Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ETS n° 108, signée à Strasbourg le 28 janvier 1981.

22 Chartre des droits fondamentaux de l'Union européenne, J.O.C.E., 18 décembre 2000, C-364/1. Cette Charte est devenue juridiquement contraignante depuis l'entrée en vigueur du Traité de Lisbonne.

23 Directive 95/46/CE du Parlement et du Conseil 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, J.O.C.E., n° L 281 du 23 novembre 1995, pp. 31 et s.

24 "In open networks such as the Internet, information accessible to the public typically cannot be kept under the control of the user who originated the data. The reason is that data can be digitally copied, stored locally, and re-entered into the Internet, often in different locations for different purposes."
(ENISA, "The right to be forgotten - between expectations and practice", 20 novembre 2012, p. 10, disponible à l'adresse https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/)

que l'on révèle à un moment de sa vie, on ne veut pas nécessairement qu'il soit accessible de manière permanente. Ceci soulève précisément la question de la reconnaissance ou non d'un droit à l'oubli.

8. Avant de se focaliser sur ce dernier point, il convient de clarifier un dernier terme. Le concept d'information personnelle ou de donnée à caractère personnel doit être entendu de manière très large. Il ne doit pas être lié à l'idée d'intimité, comme dans l'approche "classique" de la vie privée. Il signifie au contraire *n'importe quelle* information relative à une personne physique[25]. Il couvre donc les données professionnelles, les données commerciales et les données publiques.

II - Le droit à l'oubli lié à l'autonomie informationnelle

9. Ainsi que déjà évoqué[26], le droit à l'oubli a initialement été lié à l'écoulement du temps. Il est présenté aujourd'hui comme partie de l'autonomie informationnelle.

La Commission européenne a fait part de ses préoccupations à propos des problèmes soulevés par l'interaction entre les spécificités d'Internet. Une mémoire parfaite associée à la dé-contextualisation des données s'est révélée source de problèmes pour les individus. Et les utilisateurs de services de réseaux sociaux se sont plaints de ne pas être à même d'obtenir l'effacement complet de leurs données enregistrées et conservées par le fournisseur de service. Dans sa proposition de règlement général pour la protection des données[27], la Commission s'attaque à ces problèmes en garantissant notamment un droit à l'oubli digital (article 17 de la proposition de règlement[28]).

On observe que ce n'est pas tant une question d'effacement du passé qui est en jeu dans ces cas. En ce qui concerne le problème de dé-contextualisation, par exemple, il est vrai que les éléments remontés à la surface par les moteurs de recherché doivent nécessairement avoir été diffusés précédemment quelque part sur le Net. Mais « précédemment » peut signifier quelques minutes auparavant, ce qui ne correspond pas à ce qui est entendu d'ordinaire par « le passé ». Ce n'est pas la longueur du temps écoulé depuis le traitement initial des données qui importe.

Le droit à l'oubli en ce sens n'implique pas d'ailleurs l'effacement des données. Si elles demeurent dans leur contexte initial, les données ne sont pas nécessairement problématiques. On ne désire pas nécessairement leur effacement mais bien plutôt l'effacement du lien qui permet aux moteurs de recherche de sélectionner ces données durant leur « ratissage » du Web.

---

25 Voy. La définition donnée à l'article 2.a) de la directive 95/46 : « toute information concernant une personne physique identifiée ou identifiable (personne concernée) ».

26 Supra Section 1

27 Commission européenne, Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), COM(2012) 11 / 4, 25 janvier 2012

28 Cette disposition est reprise dans la présente analyse en tenant également compte des modifications adoptées par le Parlement européen (Parlement européen, Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), Compromise amendements, 7 octobre 2013). Le Conseil, pour sa part, ne s'est pas encore accordé sur un texte au moment de la remise de la présente contribution. Le trilogue devant déboucher sur un texte commun pourra encore apporter son lot de changements et d'ajustements.

Le droit à l'oubli, dans cette approche, est bien plus large qu'une préoccupation à propos du lien entre le passé et le présent. Il relève de l'autonomie informationnelle.

Quand cette autonomie est exercée par un individu à l'égard de données le concernant qu'il a lui-même diffusées précédemment, le droit à l'oubli correspond dans ce cas à un « droit de changer d'avis » et un « droit au repentir ».

10. Tous ces aspects d'un droit à ne pas voir en permanence rappeler son passé, un droit d'obtenir qu'une personne ne conserve plus ce qu'elle savait parce que ce n'est plus légitime, un droit de refuser la dé-contextualisation des données et un droit au repentir et à changer d'avis, constituent le droit à l'oubli tel que nouvellement dessiné.

Ce droit peut être abordé en tenant compte de deux situations différentes:

- Quand le traitement des données est basé sur le consentement de la personne concernée (section 3 ci-dessous)
- Et quand le traitement des données repose sur un autre fondement que le consentement (section 4 ci-dessous)

Section 3 - Le droit à l'oubli en cas de traitement de données basé sur le consentement de la personne concernée

I- Le droit à l'oubli en tant que droit au repentir et à changer d'avis

11. Un aspect du droit à l'oubli est spécifiquement lié au Web 2.0 même s'il n'est pas limité à ce contexte. Le Web 2.0 permet l'interactivité. Les utilisateurs ont la possibilité de s'exprimer, de manifester leurs idées et opinions et de diffuser des informations, des photos, des vidéos,... De nombreux services Internet emblématiques illustrent l'engouement du public pour l'interactivité : Wikipedia, Youtube et tous les sites de réseaux sociaux surpeuplés.

Mais, ainsi que dans la vie ordinaire, il arrive que vous regrettiez ce que vous avez exprimé ou diffusé grâce à cette interactivité du Web. Ou il se peut que vous changiez d'avis.

De telles situations sont particulièrement fréquentes quand l'expression est spontanée et impulsive (comme c'est souvent le cas sur les sites de réseaux sociaux). Il convient de noter que c'est la première fois dans l'histoire de la communication publique que ce type d'expression spontanée ne disparait pas mais, au contraire, demeure continuellement accessible pour le public ou pour une partie du public, longtemps après sa mise à disposition.

Le repentir ou les changements d'avis surviennent aussi souvent à l'égard d'information ou de photos partagées à un moment de la jeunesse de leur émetteur. Une fois ces jeunes devenus adultes, ils peuvent souhaiter effacer les traces de leurs activités en ligne durant leur adolescence, qu'ils viennent à considérer aujourd'hui immatures, irresponsables, incorrectes ou inconvenantes.

Mais il s'avère très difficile de réaliser cet exercice sain de nettoyage des stupidités de son passé. On a même découvert qu'il était impossible d'effacer entièrement des données une fois postées sur Facebook.[29] La Commission européenne elle-même a affirmé qu'elle « avait ainsi reçu

29 Voy. Les plaintes contre Facebook introduites par Max Schrems, un étudiant en droit autrichien, ainsi que par quelques autres, auprès de l'autorité de protection des données irlandaise (le Irish Data Protection Commissioner) à

plusieurs plaintes de personnes qui n'avaient pu récupérer des données à caractère personnel auprès de prestataires de services en ligne, telles que leurs photos, et qui ont donc été empêchées d'exercer leur droit d'accès, de rectification et de suppression. »[30]

Le droit de retrait du consentement conduisant à l'effacement des données

12. Au regard de ces difficultés, la Commission européenne a clarifié à l'article 17 de sa proposition de règlement général de protection des données, consacré au « Droit à l'oubli et à l'effacement » que les personnes concernées devraient se voir reconnaitre le droit de voir leurs données effacées lorsqu'elles ont retiré leur consentement au traitement. Cette clarification de la possibilité de retirer le consentement précédemment accordé est bienvenue étant donné que la question a suscité des discussions jusqu'à présent. L'article 7, § 3 de la proposition de règlement prévoit déjà expressément le droit de retrait de consentement à tout moment[31]. L'article 17 néanmoins stipule que ce retrait peut être considéré comme faisant partie du droit à l'oubli. Par-dessus tout, il apporte un complément d'information quant à l'effet du retrait en termes d'effacement des données (article 17, § 1er) ou d'utilisation restreinte de celles-ci (article 17, § 4).

Le texte spécifie que la suppression des données ne surviendra après le retrait du consentement que s'il n'y a pas d'autre fondement légal pour le traitement des données.

L'obligation d'effacer les données comme conséquence de l'exercice du droit de retrait du consentement et, plus largement, du droit à l'oubli est perçue comme la réponse appropriée au problème des réseaux sociaux comme Facebook qui ne suppriment pas réellement les données retirées par les utilisateurs mais qui les rendent seulement non accessibles.

Le droit à l'effacement dans les cas où l'information a été diffusée à l'initiative de la personne concernée par les données semble parfaitement logique et évident, même pour Peter Fleisher (le Global Privacy Counsel de Google) qui est pourtant un fervent opposant au droit à l'oubli. Selon lui, « Si je poste quelque chose en ligne, devrais-je avoir le droit de le retirer? Je pense que la plupart d'entre nous est d'accord sur ce point, ceci étant le cas le plus simple et le moins controversé. Si je poste une photo sur mon album, je devrais alors pouvoir la retirer plus tard si j'ai reconsidéré la chose. »[32]

---

propos d'échanges, d'informations, de messages et même d'amis conservés par Facebook longtemps après que l'utilisateur les a « supprimés », disponible à l'adresse :
http://www.europe-v-facebook.org/EN/Complaints/complaints.html. Voy. également B. Van Alsenoy, J. Ballet, A. Kuczerawy, J. Dumortier, 'Social networks and web 2.0: are users also bound by data protection regulations?', Identity in the Information Society Journal - IDIS (2009) 2, pp. 65–79.

30 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», 4 novembre 2010, COM(2010) 609 final, p. 8.

31 L'article 7, § 3, de la proposition de règlement prévoit déjà que : « La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement préalablement donné. »

32 "If I post something online, should I have the right to delete it again? I think most of us agree with this, as the simplest, least controversial case. If I post a photo to my album, I should then later be able to delete it, if I have second-thoughts about it." (P. Fleisher, "Foggy thinking about the Right to Oblivion", Blog de Peter Fleisher, 9 Mars 2011).

II- Les effets de l'exercice du droit à l'oubli

A- L'effacement des données ou...

13. L'article 17, § 1er de la proposition de règlement garantit à la personne concernée par les données, au nom du droit à l'oubli, le droit d'obtenir du responsable du traitement « l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données ». La personne concernée a donc le droit de demander que ses données à caractère personnel soient supprimées et non seulement rendues inaccessibles ainsi que la pratique des réseaux sociaux l'a montré.

La personne concernée peut aussi préférer que ses données ne soient pas supprimées mais exiger qu'elles soient transmises à un autre système de traitement automatisé (article 17, § 4, d).

14. On peut regretter que cette hypothèse de la transmission à un autre système de traitement automatisé soit la seule qui diffère de l'effacement envisagée dans le projet de règlement[33]. En effet, il peut se présenter d'autres cas où la personne concernée retirant son consentement n'a pas l'intention de voir ses données effacées :

- Ne plus être associé aux données pourrait parfois suffire. L'anonymisation des données pourrait être une réponse adéquate à une telle aspiration.
- Dans certains cas le problème découle de la diffusion publique des données, et non du traitement interne des données. La personne concernée pourrait en pareils cas souhaiter arrêter la publication des données mais accepter que les données continuent d'être conservées et utilisées par le responsable du traitement. Un accès restreint aux données pourrait conduire au même résultat. Les accès extérieurs seraient bloqués.
- La personne concernée pourrait également demander d'arrêter certaines formes de publication mais accepter d'autres formes (une personne a consenti, par exemple, d'être filmée et accepte que le film soit diffusé à la télévision un jour et une heure convenus, mais refuse de voir ce film accessible en permanence sur Internet par la suite).
- Ou encore, il se peut que la personne concernée veuille agir contre la dé-contextualisation et serait simplement heureuse de voir ses données dé-référencées, désindexées, tout lien vers elles étant supprimé. Ce serait là l'instrument adéquat contre la dé-contextualisation des données sans priver les membres du cercle initial de la possibilité d'accéder à ces données pourvu qu'elles restent au sein du cercle.

B- Information des tiers

15. « Afin de renforcer le droit à l'oubli numérique dans l'environnement en ligne »[34], l'article 17, § 2,[35] de la proposition de règlement étend le droit à l'effacement « de façon à ce que

---

33 D'autres hypothèses sont listées à l'article 17, § 4, mais aucune ne correspond au retrait de consentement.

34 Considérant 54 de la proposition de règlement.

35 L'article 17, § 2, de la proposition de énonce que "Lorsque le responsable du traitement visé au paragraphe 1 a rendu publiques les données à caractère personnel, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent

le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données, ou toute copie ou reproduction de celles-ci. Afin d'assurer cette information, le responsable des données devrait prendre toutes les mesures raisonnables, y compris les mesures techniques, à l'égard des données dont la publication lui est imputable. »[36]

Ceci a été présenté par certains commentateurs comme la réelle innovation de la proposition de règlement en ce qui concerne le droit à l'oubli. Pourtant il est à noter que cette disposition ne se distingue pas vraiment de l'article 12, c) de la directive 95/46 qui garantit que chaque personne concernée a le droit d'obtenir du responsable du traitement « c) la notification aux tiers auxquels les données ont été communiquées de [...] tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné ».

Le principe d'une obligation d'informer les personnes qui traitent des données controversées en aval du traitement initial est déjà présent dans la directive 95/46. On observe toutefois certaines divergences :

- Cette obligation n'est attachée dans la directive existante qu'à l'exercice du droit à l'effacement et non aux autres facettes du droit à l'oubli que sont le retrait du consentement et le droit d'opposition, alors que la proposition de règlement élargit le devoir d'information en aval à l'ensemble de ces facettes, ce qui est particulièrement cohérent ;
- L'article 17, § 2, stipule clairement que l'obligation d'informer découle automatiquement de l'effacement sans que la personne concernée ait à le demander, tandis que cela n'est pas clair dans la directive;
- En outre, l'article 17, § 2, vise les cas où les données ont été rendues publiques alors que l'article 12, c) concerne des données communiquées à des tiers. Le cas où le responsable du traitement communique les données à un ou plusieurs destinataires identifiés n'est a priori pas couvert par l'expression « rendre les données publiques ». Cette hypothèse tombe donc en-dehors du champ de l'article 17, § 2. On peut se demander si c'était là ce que souhaitaient les auteurs de la proposition de règlement. Cela signifie qu'il n'y aurait pas de devoir d'informer les concepteurs d'applications qui ont obtenu par contrat avec le service de réseau social l'accès aux données à caractère personnel des utilisateurs de ce service en vue de « nourrir » leur application. En fait, cela correspondrait paradoxalement aux cas où l'obligation d'informer ne soulèverait pas de problèmes majeurs de praticabilité.

Il est à noter que le Parlement européen est allé plus loin que la Commission et, plutôt qu'une simple obligation d'information des tiers à propos d'une demande d'effacement, voudrait voir peser sur le responsable du traitement le devoir de prendre toutes les mesures raisonnables pour

---

lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci."

36Considérant 54 de la proposition de règlement.

faire effacer les données, y compris par les tiers[37]. Le responsable aurait en outre l'obligation d'informer la personne concernée, si c'est possible, de ce qui aura été fait par les tiers en question[38].

Il convient de relever que la praticabilité du devoir d'information est déjà fortement contestée[39]. Il semble clair que ces obligations additionnelles paraîtront encore moins réalistes aux acteurs de terrain. Il est évident qu'une fois que les données sont rendues accessibles sur Internet, c'est un véritable défi que de savoir où les données ont été diffusées et qui est en mesure de les traiter[40]. Et entrer en contact avec toutes ces personnes pourrait se révéler vraiment difficile voire même impossible. La Commission envisage la possibilité de solutions techniques pour faire face à cette difficulté et, de façon réaliste, l'obligation pesant sur le responsable est formulée comme une obligation de moyens et non de résultat.

Le Parlement européen, quant à lui, a en fait restreint l'obligation du responsable aux seules situations où ce dernier a publié les données sans se baser sur une des justifications de traitement admises (consentement de la personne, contrat, obligation légale, intérêt public, intérêt vital ou intérêt supérieur du responsable ou du destinataire)[41].

Cette proposition du Parlement, et singulièrement la justification qui la sous-tend, démontre une approche confuse et problématique du droit à l'oubli. Ce droit (à tout le moins en ce qui concerne l'obligation en cas de publication des données) semble confondu avec le droit à l'effacement tel que perçu dans la directive 95/46[42]. Il est alors un instrument pour réagir contre le traitement illégal des données (ici la publication illégale des données). Or, le droit à l'oubli ne doit pas être limité au traitement illégal des données. Exercer ce droit à l'égard de responsables qui publient des données en se basant sur un fondement légal est parfaitement légitime. Retirer son consentement ou s'opposer à un traitement de données s'effectuent dans les deux cas à

---

37 "[The controller] shall take all reasonable steps to have the data erased, including by third parties", Parlement européen, Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), Compromise amendements, 7 octobre 2013, article 17, § 2.

38 "The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.", Ibidem. Voy. également "The rights of data subjects must be reinforced. Article 17(2) imposes an obligation of responsibility on the controller. This must be accompanied at the very least by a duty to inform regarding the action taken by third parties processing the personal data in question." Parlement européen, Comité Marché intérieur et protection du consommateur, Opinion on the Proposal for a General Data Protection Regulation, Rapporteur: Lara Comi, 28 janvier 2013, amendment 121.

39 Voy. notamment l'opinion du Contrôleur européen à la protection des données, op. cit., §§ 146-147.

40 Voy. ENISA, "The right to be forgotten - between expectations and practice", 20 novembre 2012, disponible à l'adresse https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/

41 Art. 7.2. "Where the controller referred to in paragraph 1 has made the personal data public without a justification based on Article 6(1), [...]" (Parlement européen, Compromise amendements, 7 octobre 2013). La Commission LIBE du Parlement européen avait précédemment justifié cette proposition de la sorte: "if a publication of personal data took place based on legal grounds as referred to in Article 6(1), a "right to be forgotten" is neither realistic nor legitimate. [...] This does not imply that third parties can further process published personal data if there is no legal ground for them." (Parlement européen, Commission Libertés civiles, Justice et Affaires intérieures (LIBE), Draft Report on the Proposal for a General Data Protection Regulation, Rapporteur: Jan Philipp Albrecht, 17 décembre 2012, amendments 35 and 147).

42 Voy. en outre, infra, ce qui est dit concernant le vote du Parlement européen sur les amendements de compromis modifiant le texte proposé par la Commission.

l'égard de traitements de données licites. Restreindre le droit à l'oubli au fait de réagir contre la publication illégale de ses données limiterait ce droit à un simple droit à l'effacement tel que compris dans le texte actuel de la directive. Ce serait juste un instrument pour veiller au respect de la législation.

Section 4 - Le droit à l'oubli en cas de traitement de données basé sur un autre fondement que le consentement

16. Dans les cas où le traitement des données à caractère personnel est basé sur un autre fondement que le consentement de la personne concernée, les intérêts de cette dernière protégés par le droit à l'oubli entrent en conflit avec d'autres intérêts, droits et libertés : ceux de la personne qui traite les données en cause ou d'autres personnes intéressées au traitement de ces données, ou encore certains intérêts publics. En particulier, ils se heurtent à la liberté d'expression et à la liberté de presse. Ils empiètent sur la conservation des archives, ainsi qu'on le verra dans les développements de la présente contribution portant sur les archives des journaux sur Internet[43]. Pour la même raison, le droit à l'oubli porte atteinte au devoir de mémoire. C'est un obstacle à la recherche historique. Il a aussi un impact sur la continuité des activités économiques, sur la gestion des fichiers du personnel, sur l'obligation de conserver des preuves, etc.[44] Et l'on doit aussi impérativement tenir compte de l'obligation légale de conserver certaines données à des fins de sécurité publique.

La réponse juridique face à de tels conflits consiste à mettre en balance les valeurs et intérêts concurrents en vue d'atteindre un équilibre équitable. Il n'existe en effet pas de hiérarchie prédéterminée parmi les droits de l'homme. Cela signifie que les conflits de droits ne peuvent être résolus en donnant systématiquement la priorité à un droit par rapport à un autre. La réponse à un conflit passe toujours par le test de la mise en balance. Les droits concurrents sont mis dans la balance de manière à atteindre un résultat équilibré, respectueux du principe de proportionnalité. Les restrictions encourues par la valeur sacrifiée ne doivent pas être disproportionnées par rapport au bénéfice obtenu par la valeur concurrente.

I- La mise en balance des intérêts et le droit à l'oubli du passé judiciaire

17. La signification donnée en premier lieu au droit à l'oubli est liée au passé judiciaire ou pénal d'un individu. C'est la facette la plus classique de ce droit. Ce dernier était au départ essentiellement lié à la création des archives pénales. Il a été reconnu en tant que tel par la jurisprudence de plusieurs pays, basée sur le droit à la vie privée ou sur les droits de la personnalité. Ainsi qu'évoqué dans la section 1 de la présente contribution, le droit à l'oubli, dans cette acception, est justifié par la foi en la capacité de l'être humain de changer et de s'améliorer, de même que par la conviction que l'homme ne doit pas être réduit à son passé. Une fois que

---

43 Voy Section 4. II. C

44 C. de TERWANGNE, J-Ph. MOINY, Rapport sur la consultation relative à la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, Conseil de l'Europe, juin 2011, disponible à :
http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_fr.pdf

vous avez payé votre dette, la société doit vous offrir la possibilité d'un nouveau départ sans porter toute votre vie le poids des erreurs passées.

Ce droit entre en conflit avec le droit à l'information, le temps étant le critère pour résoudre le conflit.

A- Le critère de l'actualité ou de l'intérêt historique

18. Le droit à l'oubli doit laisser la priorité aux exigences du droit à l'information quand les faits qui sont révélés présentent un intérêt d'actualité à être publiés. L'intérêt est donc lié à l'actualité des informations diffusées. Il en est ainsi lorsqu'une décision judiciaire prononcée par une cour ou un tribunal relève de l'actualité judiciaire. Il est alors légitime d'évoquer cette décision en mentionnant le nom des parties (sauf s'il s'agit de mineurs, auquel cas des règles de protection différentes s'appliquent). Mais, dès que le temps s'est écoulé et qu'il n'est plus question d'actualité, dès lors donc que les nécessités de l'information ne justifient plus une rediffusion des données, le droit à l'oubli primera sur le droit à l'information. La mention du cas pourra toujours être faite mais elle ne devrait plus inclure les noms des parties ou des données identifiantes. Ainsi, l'intérêt médiatique d'un cas fera pencher les plateaux de la balance en faveur du droit à la diffusion plutôt que du droit à l'oubli. Par contre, dès qu'il ne méritera plus de faire l'actualité, les plateaux pencheront dans l'autre sens.

Deux exceptions peuvent être admises à ceci. Cela signifie que le droit à l'information primera en dépit de l'écoulement du temps

- pour des faits appartenant à l'histoire ou concernant un sujet d'intérêt historique et

- pour des faits liés à l'exercice d'une activité publique par une personne publique.

L'intérêt historique et l'intérêt public doivent également être pris en considération pour résoudre le conflit entre le droit à l'oubli et le droit à l'information.

B- Impact des développements techniques sur le test de mise en balance: le pouvoir des moteurs de recherche

19. Les développements techniques ont radicalement modifié l'équilibre atteint auparavant entre la nécessité de diffuser l'information judiciaire et le droit individuel à l'oubli. Ainsi qu'on l'a mentionné précédemment, la moindre information peut être remontée à la surface et rassemblée avec les autres pièces du puzzle. Ceci implique un changement radical.

Il convient de citer une décision de la Cour Suprême américaine[45] prononcée il y a plus de vingt ans mais néanmoins particulièrement éclairante pour aujourd'hui, où la Cour Suprême a souligné ce changement. L'affaire concernait un journaliste qui demanda au *Federal Bureau of Investigation* l'accès aux documents concernant les arrestations, inculpations et condamnations dont firent l'objet quatre individus. Les arrestations, inculpations et condamnations sont des événements publics retranscrits dans les fichiers publics tenus par les tribunaux. Pour le seul vivant des quatre individus ciblés par le journaliste, le F.B.I. refusa de transmettre l'information qu'il détenait sous forme compilée, estimant que la communication porterait atteinte à la vie privée de l'individu en

---

45 Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

question. La Cour suprême soutint à l'unanimité cette argumentation. Elle rejeta l'argument retenu par la Cour d'appel, selon lequel il n'y a plus de « privacy interest » en présence d'informations déjà rendues publiques. Pour la Cour, il y a une importante différence entre une communication « éparpillée » de fragments d'information et la divulgation de l'information dans son ensemble.[46]

Dans le même sens, une Cour d'appel californienne affirma que « c'est la nature agrégée de l'information qui lui donne de la valeur aux yeux du défendeur ; c'est la même qualité qui rend sa diffusion constitutionnellement dangereuse »[47].

Le pouvoir des moteurs de recherche sur Internet de rassembler n'importe quelle donnée concernant un individu ciblé, à n'importe quel moment, de n'importe où, sans la moindre formalité administrative, sans révéler sa propre identité et gratuitement suscite un danger encore plus grand. Nous devons reconsidérer avec soin l'équilibre à atteindre. Concernant le point précis des données relatives au passé judiciaire, une première réponse consiste dans l'anonymisation des bases de données jurisprudentielles accessibles sur le Net[48]. Cette anonymisation est ainsi la règle aujourd'hui dans la majorité des pays européens. Cependant une autre source de sérieuse préoccupation concerne la question des archives de journaux. Ce problème fera l'objet de développements au point B ci-dessous.

II- La mise en balance des intérêts et les éléments du droit à l'oubli issus de la législation de protection des données

A- Le droit d'opposition au traitement des données

20. Certains commentateurs ont dit que le droit à l'oubli digital nouvellement revendiqué n'était peut-être seulement que la traduction « lyrique » du droit d'opposition déjà existant[49].

Un droit d'opposition est en effet déjà garanti aujourd'hui par l'article 14 de la directive 95/46. Cette disposition stipule que toute personne concernée se voit reconnaitre le droit « de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement ». Si les données sont destinées à être traitées à des fins de prospection (direct marketing), le droit d'opposition n'est en ce cas pas conditionné à la démonstration d'une justification[50].

---

46 « But the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, country archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information. » 489 U. S., 764.

47 Notre traduction: "It is the aggregate nature of the information which makes it valuable to respondent; it is the same quality which makes its dissemination constitutionally dangerous." Westbrook v. Los Angeles County, 32 Cal. Rptr. 2d 382 (Cal. App. 1994)

48 Sur cette question qui ne peut être développée davantage dans la présente contribution voy. C. de TERWANGNE, « Diffusion de la jurisprudence via Internet dans les pays de l'Union européenne et règles applicables aux données personnelles », Petites Affiches, 2005, n°194, pp. 40-48.

49 CYBERLEX, L'Association du Droit et des Nouvelles Technologies, « Contribution dans le cadre des travaux sur le droit à l'oubli numérique. L'oubli numérique est-il de droit face à une mémoire numérique illimitée? », 2010, p. 10. http://www.cyberlex.org/images/stories/pdf/contribution_cyberlex_dao.pdf

50 Art. 14, § 1, b) de la directive 95/46.

Il est à noter que le droit d'opposition, dans sa tournure donnée par l'article 19 de la proposition de règlement, présente un changement majeur en comparaison de la manière dont il est formulé à l'article 14 de directive 95/46. Les raisons que la personne concernée doit avancer lorsqu'elle désire s'opposer au traitement de ses données ne doivent plus être raisons prépondérantes et légitimes. Elles ne doivent plus que se rapporter à la situation particulière de la personne concernée.[51] Le considérant 56 l'affirme clairement: « Il devrait incomber au responsable du traitement de prouver que ses intérêts légitimes prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée. ». En conséquence, le droit d'opposition devra être plus facile à exercer pour la personne concernée. Le responsable du traitement devra au contraire démontrer, lui, des rasions prépondérantes et légitimes pour le traitement, prévalant sur les droits et intérêts de la personne concernée, s'il désire poursuivre le traitement des données. Cette inversion de la charge de la preuve doit être approuvée car le responsable est en meilleure position pour connaitre toutes les implications du traitement.

Le droit d'obtenir du responsable l'effacement des données à caractère personnel ne sera effectif qu'après avoir déterminé si les raisons de poursuivre le traitement priment ou non sur les intérêts en faveur du droit à l'oubli. Cela signifie qu'une inévitable mise en balance entre ces intérêts devra avoir lieu.

B - Exemple des archives de presse sur internet. Critères pour la mise en balance: actualité, intérêt historique et intérêt public

21. Les archives de presse sur Internet contiennent toutes sortes d'informations qui furent à un moment des nouvelles. Nombre de ces informations se rapportent à des individus. Elles ne sont pas limitées aux données judiciaires bien sûr.

Le sort des données à caractère personnel mentionnées une fois dans un journal et ensuite éternellement accessibles sur le site d'archives de ce journal soulève le problème d'un conflit potentiel entre le droit de la personne à l'oubli et la liberté de la presse.

Pour régler un tel conflit soulevé par les archives de presse sur Internet, il faut tenir compte des critères suivants mentionnés antérieurement:

- l'actualité des données,
- l'intérêt historique
- et l'intérêt public qui peuvent s'y attacher.[52]

Par définition, les archives des journaux ne sont plus supposées présenter une quelconque valeur d'actualité. Si l'on considère leur valeur historique, il faut notamment prendre en compte le fait que d'autres sources d'information existent ou non. Pour ce qui est des données judiciaires, une attention particulière doit aussi être accordée au fait qu'un appel a été introduit à l'encontre des décisions judiciaires enregistrées dans les archives de presse. Si c'est le cas, le premier jugement

---

51 L'article 19.1 de la proposition de règlement énonce: « La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à ce que des données à caractère personnel fassent l'objet d'un traitement fondé sur l'article 6, paragraphe 1, points d), e) et f), à moins que le responsable du traitement n'établisse l'existence de raisons impérieuses et légitimes justifiant le traitement, qui priment les intérêts ou les libertés et droits fondamentaux de la personne concernée.. »

52 Sur ces critères, voy. Cour eur. D.H., Osterreichischer Rundfunk, 7 mars 2007.

pourrait être conservé mais devrait être accompagné d'une notice spécifiant que la décision est en cours de révision.

A l'occasion de l'affaire *Times Newspapers*, la Cour européenne des droits de l'homme a apporté un éclairage très intéressant concernant la manière dont le test de mise en balance devrait être mis en œuvre. Même si le droit à l'oubli n'était pas en jeu dans ce cas[53], la déclaration de la Cour pourrait utilement être appliquée aux hypothèses impliquant un conflit entre la liberté de presse et le droit à l'oubli en présence d'archives de presse publiquement accessibles. La Cour a affirmé que le maintien des archives présentait un grand intérêt pour la société mais que cela correspondait néanmoins à un rôle accessoire de la presse. En tant que tel, cet aspect de la liberté de presse pèse moins lourd quand on effectue la mise en balance avec une autre valeur que lorsqu'est en jeu la fonction principale de la presse, celle du fameux chien de garde. La Cour dit qu'elle souscrit à la thèse de la société requérante « selon laquelle la mise à disposition d'archives sur Internet contribue grandement à la préservation et à l'accessibilité de l'actualité et des informations. Les archives en question constituent une source précieuse pour l'enseignement et les recherches historiques, notamment en ce qu'elles sont immédiatement accessibles au public et généralement gratuites. En conséquence, la Cour estime que si la presse a pour fonction première de jouer le rôle de « chien de garde » dans une société démocratique, la fonction accessoire qu'elle remplit en constituant des archives à partir d'informations déjà publiées et en les mettant à la disposition du public n'est pas dénuée de valeur. Cela étant, les Etats bénéficient probablement d'une latitude plus large pour établir un équilibre entre les intérêts concurrents lorsque les informations sont archivées et portent sur des événements passés que lorsqu'elles ont pour objet des événements actuels ».[54]

22. Contrairement à l'article 17 de la proposition de règlement général sur la protection des données qui ne prévoit que l'effacement des données et l'arrêt de leur diffusion, on peut envisager différents résultats d'une mise en balance concernant le droit à l'oubli (voy. le point 4.4. Les effets de l'exercice du droit à l'oubli). Ici par exemple, le résultat pourrait être l'obligation d'effacer les données identifiantes d'un article dans les archives de presse publiquement accessibles sur Internet. Une version non-expurgée serait conservée avec un accès restreint (pour des finalités de recherches, notamment). Ou le résultat pourrait être l'exigence que des informations additionnelles soient liées aux données (un avertissement ou le point de vue de la personne concernée, par exemple). La conclusion devrait toujours être atteinte au cas par cas.

Il convient d'avoir à l'esprit que ce problème est principalement lié à l'accessibilité publique via Internet de l'information controversée L'équilibre atteint sur le Web ne doit pas nécessairement correspondre à ce qui est fait dans les formats classiques. Certaines solutions consisteront très vraisemblablement à donner la priorité à la liberté de la presse, et aux intérêts historique, pédagogique et public pour des archives se présentant dans des formats non accessibles sur le Net. Par contre, le préjudice découlant de la disponibilité éternelle et universelle des données via Internet sera bien plus souvent considéré comme disproportionné que le dommage résultant d'une publicité locale sujette à des démarches.

---

53 Il s'agissait d'une question de diffamation potentielle liée à des informations disponibles dans les archives du Times sur Internet; les articles originaux avaient été présents sans notice avertissant qu'ils faisaient l'objet d'une action en diffamation.

54 Cour eur. D.H., Times Newspapers Limited (Nos. 1 and 2) v. the United Kingdom, 10 Mars 2009, req. n° 3002/03 et n° 23676/03, § 45 (c'est nous qui soulignons).

C - L'obligation de supprimer des données à caractère personnel découlant du principe de finalité

23. Les hypothèses de droit à l'oubli présentées ci-dessus sont laissées à l'initiative de la personne concernée. Il existe une autre manière de réaliser le droit à l'oubli qui n'exige aucune initiative de la personne concernée. Pour bénéficier du droit à l'oubli découlant du principe de finalité, la personne concernée ne doit faire aucun effort. C'est au responsable du traitement qu'il revient de veiller à ce que les données à caractère personnel soient effacées quand la finalité du traitement est atteinte ou ne justifie plus de conserver les données.

Le principe de finalité est un des principes de base du régime de protection des données. Ce principe spécifie que les données à caractère personnel doivent être traitées pour une finalité déterminée, légitime et transparente. Le droit à l'oubli découle directement du principe de finalité car, selon une application de ce principe, le responsable du traitement peut conserver les données « sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. »[55] Cela signifie que les données à caractère personnel peuvent être conservées en tant que telles tant que cela est justifié pour réaliser la finalité du traitement. Elles doivent être soit anonymisées, soit supprimées une fois que le but a été atteint ou aussitôt qu'il n'y a plus de nécessité de garder le lien avec des personnes identifiables pour atteindre ce but.

Les personnes concernées se voient octroyer le pouvoir de vérifier le respect de cette règle.

D- Le droit à l'effacement sensu stricto

24. Le droit à l'effacement fait partie de l'actuel article 12, b) de la directive 95/46 qui prévoit que toute personne concernée a le droit d'obtenir du responsable du traitement « l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données ». L'effacement ou le verrouillage des données est, dans la directive 95/46, une façon pour la personne concernée d'agir contre le non-respect des règles de protection. Importer ce droit, comme cela est fait à l'article 17 de la proposition de règlement, dans une disposition consacrée au droit à l'oubli a justifié ces mots du considérant [53] de ce texte qui précise que : « Toute personne devrait avoir le droit de [...] disposer d'un 'droit à l'oubli numérique' lorsque la conservation de ces données n'est pas conforme au présent règlement ».

On a vu dans les points qui précèdent que la possibilité de retirer son consentement et celle de s'opposer au traitement des données sont accordées à la personne concernée à l'égard de traitements licites de leurs données. Le contexte ne s'apparente pas du tout à celui dans lequel intervient le droit à l'effacement des données *sensu stricto* qui est celui d'un traitement de données non conforme. A la différence du droit au repentir et du droit d'opposition, le droit à l'effacement est un instrument en vue de faire respecter le régime de protection. (Voy. également les remarques conclusives de la présente contribution.)

---

55 Art. 6, § 1, e) de la directive 95/46.

III - Les effets de l'exercice du droit à l'oubli

A- L'effacement, l'anonymisation ou le verrouillage, ou...

25. Au vu des différentes facettes du droit à l'oubli se trouvant dans le régime juridique de la protection des données, ce droit peut induire selon l'hypothèse l'obligation de supprimer les données (disparition des données elles-mêmes) ou de les anonymiser (disparition des éléments identifiants[56]) ou l'obligation de les verrouiller. Le terme « verrouiller » a été pointé comme étant équivoque par les auteurs de la proposition de règlement[57] qui lui ont préféré l'expression « limiter le traitement », qui n'est pas totalement plus claire... Le paragraphe 5 de l'article 17 de la proposition de règlement explicite toutefois que les données dont le traitement est limité « ne peuvent être traitées, à l'exception de la conservation, qu'à des fins probatoires, ou avec le consentement de la personne concernée, ou aux fins de la protection des droits d'une autre personne physique ou morale ou pour un objectif d'intérêt général ». A part donc la conservation des données, aucune opération ne peut plus être réalisée sur ces données, sauf dans des circonstances très limitées.

26. Les mêmes commentaires que ceux concernant les effets du retrait de consentement peuvent être faits ici. Notamment le fait que pour ces autres hypothèses d'exercice du droit à l'oubli, différents résultats que ceux mentionnés ci-dessus pourraient également être envisagés qui permettraient de mieux respecter le principe de proportionnalité :

- l'accès restreint aux données
- l'arrêt de toute diffusion des données
- la suppression de tout lien vers les données et de tout référencement pour les moteurs de recherche
- d'autres formes de publicité (offre la possibilité d'opter pour une forme de publicité qui respecte le principe de proportionnalité plutôt que pour une autre forme qui induirait un dommage trop sévère au regard des bénéfices engrangés pour les valeurs concurrentes)
- l'adjonction d'une information supplémentaire aux données (un avertissement ou le point de vue de la personne concernée, par exemple).

Cette liste de solutions nuancées pour l'exercice du droit à l'oubli devrait être disponible tant pour la personne concernée que pour le responsable du traitement et pour l'autorité de protection ou le juge potentiellement invités à déboucher sur un résultat équilibré en cas de désaccord entre les deux parties.

Le législateur appelé, lui, à réaliser *a priori* et non *a posteriori* la mise en balance, au moment où il élabore une loi faisant entrer en jeu des intérêts concurrents (en matière de sécurité publique, par exemple, de santé publique, de protection de la jeunesse, de lutte contre le surendettement, etc.) devrait pouvoir envisager, lui aussi, des solutions proportionnées et ne pas se trouver devant la seule alternative « conserver ou effacer ».

---

56 Il convient d'être conscient des limites des processus d'anonymisation et des risques existants de « désanonymisation ». Ces limites et problèmes ne peuvent faire l'objet de davantage de développements dans la présente contribution.

57 Exposé des motifs de la proposition de règlement, p. 10 : « [L'article 17] intègre aussi le droit de limiter le traitement dans certains cas, en évitant le terme équivoque de 'verrouillage' ».

B- Information des tiers

27. Le raisonnement élaboré pour le cas du retrait de consentement est entièrement valable pour les autres fondements du droit à l'oubli.[58]

Section 5- Droit à la suppression automatique des données dans l'environnement électronique – droit à l'oubli par défaut

28. En réponse aux nouveaux développements de services Internet et à la situation problématique induite par les spécificités d'Internet relevées au point S2 de cette contribution, la même proposition a été formulée dans différents cercles politiques, institutionnels ou académiques, pour accorder aux personnes concernées un droit automatique à l'oubli après l'expiration d'un certain délai.

Le Contrôleur européen à la protection des données, notamment, a proposé d'élargir le droit à l'oubli existant de manière à garantir que l'information disparaisse automatiquement après un certain délai, même si la personne concernée ne réalise aucune démarche ou n'est pas même au courant que des données la concernant étaient conservées.[59] Le Vice-Secrétaire Général du Conseil de l'Europe a atteint la même conclusion: "The increase in storage and processing capacities enables information concerning an individual to circulate within the network, even though it may no longer be valid. This makes the current principles of accuracy and proportionality of data obsolete. *A new right to oblivion or automatic 'data erasers'* would enable individuals to take control over the use of their own personal data."[60] La Vice-Présidente de la Commission européenne, V. Reding, a dit à son tour: "I want to introduce the 'right to be forgotten'. Social network sites are a great way to stay in touch with friends and share information. But if people no longer want to use a service, they should have no problem wiping out their profiles. The right to be forgotten is particularly relevant to personal data that is no longer needed for the purposes for which it was collected. *This right should also apply when a storage period, which the user agreed to, has expired.*"[61]

Ces propositions similaires reviennent à attribuer une sorte de date d'expiration aux données, sans besoin de procéder à une analyse préliminaire au cas par cas. Un certain délai pourrait être fixé, par exemple, pour les données conservées sur un équipement terminal comme un appareil ou un ordinateur mobiles: les données seraient automatiquement supprimées ou boquées après

---

58 Voy Section 3/II .*supra*

59 Contrôleur européen à la protection des données, avis du 14 janvier 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée - «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», J.O. C 181/01, 22 juin 2011, pp. 1 et s, § 85.

60 Conseil de l'Europe, Vice-Secrétaire Général, « Speaking Points for the Opening the 21st T-Pd Bureau Meeting", Strasbourg, 15novembre 2010.
http://www.coe.int/t/dghl/standardsetting/dataprotection/151110%20DSG%20speaking%20notes%20data%20protection%20meeting%20T-PD.pdf (c'est nous qui soulignons).

61 V. REDING, "Why the EU needs new personal data protection rules?"
The European Data Protection and Privacy Conference, Bruxelles, 30 novembre 2010,
http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700 (c'est nous qui soulignons).

l'écoulement de la période prévue si l'équipement n'est plus en la possession de son propriétaire initial.

Ce système est déjà d'application dans certains Etats pour certains fichiers ou registres tels que les fichiers pénaux et les registres de police. Cela rencontre ce que la Cour européenne des droits de l'homme a souligné dans l'affaire *Rotaru*: des données appartenant au lointain passé d'un individu suscitent une préoccupation particulière au regard de la vie privée protégée par l'article 8, § 1er de la Convention européenne des droits de l'homme. Elles ne devraient pas être conservées sans procéder à une analyse très stricte de la nécessité de cette conservation par rapport aux exigences démocratiques.[62]

L'automaticité de la suppression ou de l'interdiction de toute utilisation devrait être traduite en une configuration « vie privée par défaut » du traitement de données. En ce sens, à côté du droit de faire effacer ses données sur demande, le droit à l'oubli pourrait prendre la tournure d'une règle de protection des données par défaut.

Un mécanisme technique devrait donc prévoir que la conservation des données se termine automatiquement dès que le temps nécessaire pour atteindre la finalité annoncée est passé.

De telles possibilités de mettre en place un système automatique de destruction des données avec le consentement de la personne concernée existent déjà. A titre d'illustration d'un système de ce type, le logiciel X-Pire a été lancé en Allemagne[63]. Il permet aux utilisateurs d'attacher une date d'expiration digitale aux images enregistrées sur des sites de réseaux sociaux comme Facebook.

29. Il est clair que cette voie technique pour permettre le droit à l'oubli ne peut offrir une réponse adéquate dans toutes les circonstances où la personne concernée souhaiterait exercer son droit à l'oubli. Tout d'abord, parce que des cas comme le retrait du consentement et l'opposition au traitement des données ne peuvent être prévus et prendre la forme d'une date d'expiration systématique. Ensuite, parce que la personne concernée ne veut pas nécessairement voir ses données effacées. Elle peut préférer demander d'arrêter de diffuser les données, par exemple (voy. *supra*).

Cela étant, une réponse technique comme celle évoquée ici contribuerait à faire pencher la balance en faveur de la personne concernée dès lors qu'elle bénéficierait de la protection sans avoir à prendre d'initiative. Ceci est particulièrement important dans un contexte aussi opaque que celui d'Internet. De nombreux traitements de données survenant dans cette sphère se font totalement à l'insu des personnes concernées. Il est illusoire dans ce cas de garantir aux individus un droit qu'ils ne penseraient jamais à utiliser.

Conclusion

30. Le droit à l'oubli tel qu'il se dessine aujourd'hui présente différentes facettes. Il couvre tout à la fois

- le droit au repentir et à changer d'avis à l'égard de ce que l'on a diffusé auparavant ou accepté que l'on fasse avec ses données ;

---

62 Cour eur. D.H., Rotaru c. Roumanie, 4 mai 2000, req. no 28341/95. Voy. Aussi l'opinion concordante du Juge Wildhaber à laquelle se sont ralliés les juges Makarczyk, Türmen, Costa, Tulkens, Casadevall et Weber.
63 http://www.x-pire.de/index.php?id=6&L=2

- le droit de ne pas voir en permanence rappeler son passé, de ne pas voir son passé encombrer le présent et hypothéquer l'avenir ;
- le droit d'obtenir qu'une personne ne conserve plus ce qu'elle savait parce que ce n'est plus légitime, le principe de finalité ne le justifiant plus ;
- le droit de refuser la dé-contextualisation des données en luttant principalement contre la puissance des moteurs de recherche sur Internet, tout en admettant éventuellement que les données demeurent dans leur contexte initial.

Ces différentes facettes du droit à l'oubli trouvent une expression et une protection juridiques basées sur le droit au respect de la vie privée et, singulièrement, sur l'autonomie informationnelle qui est aujourd'hui attachée à ce droit.

Le droit à la protection des données à caractère personnel donne forme à cette autonomie informationnelle. Il contient les ingrédients qui donnent corps aux différentes facettes du droit à l'oubli, qu'il s'agisse

- du droit de retrait du consentement sur lequel se fondait la diffusion ou le traitement des données,
- du droit d'opposition au traitement des données,
- du devoir de suppression ou d'anonymisation des données une fois la finalité de leur traitement atteinte et ne justifiant plus leur conservation sous une forme personnalisée,
- du droit à l'effacement des données dont le traitement est non conforme aux exigences de protection des données.

31. Les effets de l'exercice du droit à l'oubli ne devraient pas être abordés de façon binaire et être réduits à l'alternative « effacer ou conserver les données ». C'est pourtant ce type d'alternative qui est proposée dans le texte de la proposition de règlement général sur la protection des données de la Commission européenne[64], même si une solution de « limitation du traitement » est aussi proposée, très réduite au demeurant. La réduction du droit à l'oubli à un droit à l'effacement est encore plus nette dans la position adoptée par le Parlement européen.[65] Au terme du vote de cette Assemblée sur un texte de compromis modifiant la proposition de la Commission, l'article 17 dédié au « droit à l'oubli numérique et à l'effacement » voit son intitulé réduit au seul « droit à l'effacement ». Les intenses discussions qui eurent lieu dans cet hémicycle, nourries d'impressionnantes contributions de lobbyistes ayant assailli en nombre les parlementaires appelés à se prononcer, ont conduit finalement à la suppression de la notion de « droit à l'oubli » au sein du texte, pour n'en garder que la facette de l'effacement. Cet épisode n'est certes qu'un stade du processus législatif européen et on ne saurait préjuger de la tournure que prendra la version définitive du texte s'il aboutit un jour.

Que le droit à l'oubli ne soit pas (comme c'est en fait le cas aujourd'hui) ou plus (selon la suite du processus législatif européen) consacré en tant que tel dans la règlementation de la protection des données à caractère personnel n'est pas un mal irrémédiable, étant donné que tous les ingrédients qui lui donnent une forme juridique se trouvent par ailleurs dans cette règlementation. Il perdrait assurément la visibilité que la Commission tente de lui donner et son usage par les individus

64 Article 17 de la proposition de règlement, précité.

65 Parlement européen, Compromise amendements, précités.

confrontés à des difficultés liées à leurs données en circulation sur Internet n'en serait pas facilité. Mais le droit au repentir via le retrait de consentement, le droit d'opposition et le droit à l'effacement seraient tout de même à la disposition de toute personne concernée, comme ils le sont déjà.

32. Les résultats de l'exercice du droit à l'oubli devraient être bien plus nuancés que simplement obtenir l'effacement des données ou en imposer un traitement limité. Nous avons vu *supra* qu'en vue notamment d'atteindre un équilibre équitable entre les valeurs concurrentes, ce droit à l'oubli pourrait déboucher sur le droit à l'effacement mais également sur le droit à l'anonymisation (n'effacer que les données identifiantes[66]) ou sur le droit d'effacer le lien électronique vers les données (dans le but de lutter efficacement contre la dé-contextualisation des données tout en les maintenant accessibles dans les cercle et contexte originaux), ou sur le droit de restreindre la diffusion (sur des réseaux sociaux, par exemple). Cette dernière voie de réalisation du droit à l'oubli pourrait signifier pour le contrôleur l'arrêt de toute diffusion ou pour la personne concernée le choix de certaines formes de publicités plutôt que d'autres.

33. Le devoir d'agir en aval de l'exercice de ces facettes du droit à l'oubli, soit en informant les tiers, soit en veillant à ce qu'ils effacent eux aussi les données contestées, est logique et souhaitable, même s'il soulève de sérieuses questions de praticabilité en présence d'une diffusion de données sur Internet. Ce devoir qui était déjà partiellement inscrit dans la directive 95/46 se retrouve dans la proposition de règlement à la fois plus largement (il s'étend à toutes les facettes du droit à l'oubli et non pas seulement au droit à l'effacement des données) et plus restrictivement (selon la version du Parlement, il ne s'applique qu'en cas de diffusion illégitime des données). Quoi qu'il en soit, il s'agit là d'un instrument opportun dans le contexte en ligne caractérisé par sa radicale opacité. Là où ce sera raisonnablement réalisable, le responsable du traitement devra informer les utilisateurs avals. Il a plus de chance de connaitre ces personnes ou d'entrer en contact avec elles que les personnes concernées par les données contestées, spécialement s'il a un lien contractuel avec elles.

66 La présente contribution ne peut s'étendre sur les limites que connait aujourd'hui le processus d'anonymisation au vu des pratiques croissantes de brassage et de croisement de grandes quantité de données qualifiées d'anonymes.

CHAPITRE 2

Droit à l'oubli numérique et droit au respect de la vie privée attention un droit peut en cacher un autre[1] !

1. L'émergence des traces numériques. L'usage des nouvelles technologies par l'internaute révèle aujourd'hui les traits de sa personnalité. Les cartes à puces, les téléphones portables, les tablettes mettent en effet à jour de nombreuses traces numériques qui sont autant de fragments de personnalités. Quelques exemples permettent de s'en convaincre. Nos cartes d'abonnements pour des déplacements en vélo ou en métro révèlent ainsi précisément lieu de départ et d'arrivée. Ce traçage se poursuit avec la géo-localisation de nos *smartphone* ou nos navigations sur l'Internet en raison notamment des *cookies* qui représentent, comme on le sait, des petits fichiers qui s'activent sur nos disques durs au moment des requêtes. Quiconque a acheté un billet d'avion pour *Bucarest* ou *Lisbonne* s'est vu proposer hôtels ou restaurants dans ces capitales. Cette économie de la traçabilité fait le bonheur de certains opérateurs économiques comme les régies publicitaires qui sondent nos comportements pour proposer des produits commerciaux ciblés. Les pratiques dites du *scoring* ou de «segmentation comportementale » poursuivent la même finalité. Ces pratiques consistent, pour les banques, sur la base de critères déterminés, à faire entrer leurs clients dans tel ou tel « segment ». Elles ont pour but d'évaluer les risques qui s'attachent à chacun d'eux dans l'octroi d'un crédit, ainsi que, subsidiairement, de pouvoir leur proposer les produits et services les plus adaptés (où l'on retrouve les finalités de la publicité ciblée).

2. Les difficultés de protection de ces fragments de la personnalité. Cette ombre numérique ne peut être saisie par le droit au respect de la vie privée[2]. Nous sommes en effet en présence d'informations personnelles. Or l'information personnelle et la vie privée ne coïncident pas nécessairement. Si tout élément de la vie privée peut être traité comme de l'information personnelle[3], l'inverse n'est pas vrai. Nombreuses sont en effet les informations personnelles qui ne sont pas couvertes par le droit au respect de la vie privée. L'information peut être publique, comme c'est le cas par exemple, de nos adresses dans l'annuaire[4]. Elle peut aussi être jugée

---

1par Jean-Michel Bruguière, Professeur Université Grenoble Alpes, directeur du Centre universitaire d'enseignement et de recherche en Propriété intellectuelle (CUERPI)

Les pages qui suivent sont en partie extraites d'un ouvrage à paraître aux éditions Ellipses consacré aux droits de la personnalité.

2 Voir sur ce point J. Rochfeld La vie tracée ou le code civil doit-il protéger la présence numérique des personnes ? Mélanges Jean Hauser LexisNexis Dalloz 2012 p. 619.

3 Nos situations matrimoniales comme médicales peuvent être traitées comme des informations personnelles. De la même manière l'image de la personne a pu être traitée comme une donnée personnelle. Trib. gr. inst. Privas, 3 septembre 1997, Les Petites Affiches du 11 novembre 1998, p. 19, note Jean Frayssinet

4 Sur cette question cf. J.-M Bruguière Les données publiques et le droit, Litec 2002 n°9

anodine au sens de la décision de la Cour de cassation du 3 avril 2002[5], « il n'y a pas d'atteinte à la vie privée lorsque les prétendues révélations ne sont que la relation de faits publics ou ne présentent qu'un caractère anodin ». Ces informations personnelles ne peuvent donc être appréhendées par le droit au respect de la vie privée. La loi informatique fichiers et libertés est plus accueillante grâce à l'interprétation extensive de la CNIL ou du juge. A leur égard, le Conseil d'État a énoncé que si le segment « ne constitue pas à lui seul une information nominative, il le devient dès lors qu'il est associé à une personne identifiée ou indirectement identifiable et figure dans un traitement automatisé »[6]. Cette approche segmentée de la personnalité des individus est tombée ainsi sous la coupe de la protection des données à caractère personnel. Force est de constater toutefois que cette tendance n'est pas achevée[7].

3. Consécration d'un « droit à l'oubli numérique ». Jurisprudence. L'on comprend dans ces conditions pourquoi un droit à l'oubli numérique est aujourd'hui mis en avant. Forçant un peu les textes certains juges[8] n'ont pas hésité d'observer que « si aucune norme n'édicte au profit des personnes concernées un droit à l'oubli, de nombreuses dispositions légales consacrent un tel principe, telles les règles générales qui régissent les traitements de données à caractère personnel, l'effacement de certaines condamnations du casier judiciaire, la réhabilitation, l'impossibilité de rapporter la preuve d'un fait diffamatoire vieux de plus de dix ans quand l'imputation ne relève pas d'un débat public, la prohibition de principe du rappel de condamnations amnistiées quand ces dernières ne touchent pas un homme public, la prescription de l'action politique ou des actions civiles en toute matière sauf les crimes contre l'humanité… »[9].

4. Consécration d'un « droit à l'oubli numérique ». « Loi ». Sans aller solliciter le droit du casier judiciaire, la prescription pénale ou l'*exceptio veritatis*, force est de reconnaître qu'aucun texte ne reconnaît aujourd'hui ce droit à l'oubli. Les choses seront différentes demain avec le droit à l'oubli numérique. Une proposition de Règlement sur les données personnelles du 25 janvier 2012 institue ainsi dans son article 17, comme d'autres textes dans le passé[10], un « droit à l'oubli numérique et à l'effacement »[11]. L'internaute a ainsi « le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel le concernant et la diffusion de ces données » pour plusieurs raisons. Il est possible tout d'abord que « les données ne sont plus

---

5 Cass. civ. 1° 3 avril 2002 Bull. civ. I n°110

6 CE 7 juin 1995 AJDA 1996 p. 162 note J. Frayssinet

7 Voir ainsi les propositions de M. Merzeau, L. Merzeau, De la surveillance à la veille in R. Damien et P. Mathias (ss. dir.), Internet et la société de contrôle : le piège ? Cités 2009/3 n°39 p. 79 visant à mettre en place « des protocoles garantissant une plus grande étanchéité des données (…), l'individu » pouvant « gérer lui-même son portefeuille d'identités en cloisonnant ses registres de présence ».

8 Certains en effet car tous n'adoptent pas une telle position. Voir ne ce sens TGI Paris 14 janvier 2013 n°RG 11/03875 qui souligne clairement que le droit à l'oubli (ici non numérique) n'existe pas.

9 TGI Paris ord. réf. 25 juin 2009 n°RG 09/55437. Pour la petite histoire, le magistrat ayant rendu cette décision, Joël Boyer, a rempli auparavant les fonctions de secrétaire général de la CNIL. Ceci explique cela.

10 Proposition de loi du Sénat n°93, 2009-2010 et pour un commentaire A. Favreau Chronique Droit de l'internet (dir. J.-M Bruguière et V. Fauchoux), RLDC 2010 n°70 p. 76

11 Encore que ce droit, il est important de la souligner, est aujourd'hui plus simplement désigné par droit à l'effacement dans sa dernière mouture. Le 21 octobre 2013, le Parlement européen a en effet par le biais de la Commission « Libertés civiles, justices et affaires intérieures » voté un nouveau projet de règlement visant à renforcer les droits du citoyen.

nécessaires au regard des finalités pour lesquelles elles ont été collectées et traitées » (article 17 & 1 a). La personne, ensuite, peut retirer « son consentement sur lequel est fondé le traitement le traitement » ou « lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement de donnée (article 17 & 1 b). Enfin le droit d'oubli joue lorsque la personne s'oppose au traitement (article 17 & 1 c), en vertu d'une décision définitive d'une juridiction ou d'une autorité de contrôle (d) ou lorsque les données ont été traitées de façon illégale (e).

5. Opportunité et signification de la consécration d'un « droit à l'oubli numérique ». La dénomination de ce « nouveau » droit intrigue car si l'on veut bien laisser de côté les slogans législatifs, ce soit disant « droit à » l'oubli numérique est en réalité en grande partie un droit à l'effacement des données[12]. La nature de ce droit à l'oubli numérique (droit subjectif ? Droit objectif ?) est tout autant incertaine comme nous allons le voir. En bref et sans *a priori*, nous devons, tout d'abord, vérifier l'opportunité de la consécration ce « droit à » l'oubli numérique (1) et, ensuite, nous interroger sur le sens de son introduction dans notre système juridique (2). Nous allons voir que le droit à l'oubli n'apporte en réalité pas grand-chose, si ce n'est (mais peut-être est-ce déjà beaucoup…) de révéler les limites du droit au respect de la vie privée à appréhender certaines difficultés d'utilisation de l'information dans l'économie numérique. Un autre droit, le droit au respect des informations personnelles, serait peut être mieux à même de défendre les fragments de sa personnalité. En d'autres termes, attention car un droit peut en cacher un autre !

Le droit à l'oubli est un droit à oublier (1)
Le droit au respect des informations personnelles est un droit à consacrer (2).

Section 1 - Le droit a l'oubli : un droit à oublier

6. Pulvérisation des droits subjectifs, caractère absolu…critiques inopérantes. Le droit à l'oubli numérique fait aujourd'hui l'objet de discussions doctrinales. Ses défenseurs n'ont jamais véritablement expliqué ce qu'il désignait concrètement, ni ce qu'il ajoutait aux prérogatives consacrées dans la loi informatique, fichiers et libertés. Ses détracteurs soulignent généralement qu'il participe du mouvement de « pulvérisation des droits subjectifs » dénoncé par Carbonnier[13] et surtout qu'il n'est pas acceptable eu égard à son caractère absolu. L'introduction d'un nouveau droit subjectif ne devrait pas inquiéter s'il répond bien à un besoin social précis. Il en est de même de son caractère absolu. Tous les droits subjectifs, à commencer par le plus complet d'entre eux, le droit de propriété, comportent en effet des limites. Il n'y a pas de raison de décider autre chose pour le droit à l'oubli en présence notamment de la liberté d'expression ou de la liberté du commerce.

---

12 En grande partie car s'opposer à un traitement n'est pas demander l'effacement des données. Rappelons encore une fois que le projet de Règlement dans sa dernière mouture ne vise plus le droit à l'oubli mais un droit à l'effacement. (Right to erasure). Sur ce point essentiel cf. J.-M Bruguière, « Le droit à » l'oubli numérique : un droit à oublier, D. 2014 p. 299.

13 J. Carbonnier Droit et passion du droit sous la V république, Champs Flammarion 2006

Les critiques à apporter à ce droit à l'oubli numérique ne tiennent donc pas à ces deux points. Elles découlent plutôt selon nous, d'une part, du caractère fuyant de l'objet du droit (I) et d'autre part, de sa nature imprécise (II).

I- Un objet fuyant

7. L'oubli collectif et l'oubli individuel dans le droit. L'appréciation de l'objet du droit à l'oubli nécessite en premier lieu que l'on rappelle la place que l'oubli occupe dans notre droit. A l'analyse, l'oubli dans le droit comporte deux facettes, l'une est collective, l'autre individuelle. Seule la seconde est en cause dans le droit à l'oubli numérique. D'un point de vue collectif, l'oubli est synonyme de mémoire et cette mémoire, pour le législateur, peut être un devoir. Notre déclaration des droits de l'homme ne pose-t-elle pas dès sa première phrase que « l'ignorance, l'oubli ou le mépris des droits de l'homme sont les seules causes des malheurs publics » ? D'un point de vue individuel, l'oubli peut aussi préserver la personne d'un passé qu'elle souhaite taire, du moins ne plus voir évoquer. Kayser a admirablement mis en valeur cette dimension : «L'oubli est une valeur essentielle, il tient à la nature même de l'homme et refuser un droit à l'oubli c'est nourrir l'homme de remords, qui n'a d'autre avenir que son passé, dressé devant lui comme un mur qui bouche l'issue»[14]. La formule du « droit à l'oubli », que certains attribuent à Lyon-Caen dans le commentaire de l'affaire Landru[15], est lancée. C'est donc l'objet de ce droit individuel, dans l'univers numérique, qu'il faut savoir cerner.

8. La chimère de l'oubli. L'oubli, pour aller à l'essentiel, est un objet de droit particulièrement fuyant. Factuellement l'oubli est en effet une chimère. Les adeptes du « vivons heureux, vivons cachés » éprouveront beaucoup de difficultés à dissimuler les fragments de leur personnalité sur l'internet. Certains ne souhaitent d'ailleurs nullement vivre dans l'oubli, exposant tout au contraire toutes les facettes de leur vie privée[16]. En droit, l'oubli est un objet difficilement opératoire. L'oubli est en effet une quête juridique aussi difficile à atteindre que le bonheur, par exemple, que l'on trouve visé dans la constitution américaine.

9. Droit à l'oubli et droit à l'effacement des données personnelles. Le droit à l'oubli numérique renvoi en réalité au droit de demander l'effacement des données personnelles. C'est du moins ainsi que le projet de Règlement données personnelles l'envisage désormais à l'article 17 (*right to erasure*). En l'état de notre droit positif, ce droit à l'effacement passe par le droit d'accorder des mesures de désindexation sur le fondement du droit d'opposition de l'article 38 de la loi informatique fichiers et libertés. La désindexation par décision judiciaire suppose un « motif légitime »[17] qui se caractérisera par une atteinte à l'honneur, une atteinte à la dignité ou une atteinte à la vie privée comme cela a été jugé plusieurs fois en France. *Google* a été ainsi condamné à désindexer le nom patronymique et le prénom d'une femme qui avait par le passé tourné dans

---

14 P. Kayser, La protection de la vie privée, PUAM 3° éd. 1995

15 Note sous TGI Seine 14 octobre 1965 JCP 1966, II, 14482

16 Non sans revendiquer la protection des données personnelles, ce que l'on désigne par privacy paradox

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. »

des films pornographiques[18]. La même entreprise a du cesser l'affichage dans *Google Images*, pendant 5 ans, de neuf clichés, correspondant à des extraits de scènes sexuelles captées à l'insu de Max Mosley, l'ex-patron de la Fédération internationale de l'automobile, qui avaient été publiées par le journal britannique « News of the World » sur son site Internet[19]. Nous avons vu plus haut que le droit à l'effacement pouvait être demandé dans plusieurs situations différentes : retrait du consentement, expiration du délai de conservation des données...Encore faut-il préciser que ce droit à l'effacement n'existe pas véritablement. La désindexation à laquelle l'on parvient *in fine* n'entraine pas la disparition de l'information qui peut toujours être trouvée sur l'Internet. Tout au plus y a-t-il aménagement de l'accessibilité par les mots clés dans les moteurs de recherche[20].

10. Droit à l'effacement des données personnelles. Décision de la Cour de justice de l'Union européenne du 13 mai 2014. La solution adoptée par la Cour de justice de l'Union européenne le 13 mai 2014[21] confirme en tous points cette analyse. Les faits à l'origine de cette décision sont les suivants. Une personne physique de nationalité espagnole se plaignait que Google affichait, parmi les résultats de son moteur de recherche, des liens vers deux pages d'un quotidien ibérique datant de 1998 faisant état de certaines dettes qu'il avait à l'époque envers la sécurité sociale espagnole. Selon cet internaute, le référencement de ces deux articles par Google ne se justifiait nullement au regard de l'ancienneté de l'affaire. Après une démarche infructueuse auprès du journal et de Google, l'internaute décide de saisir l'autorité espagnole de protection des données à caractère personnel. Celle-ci rejette sa demande contre le journal qui avait publié les informations en toute légalité, étant donné que la publication avait eu lieu sur ordre du ministère du Travail et des Affaires sociales et avait eu pour but de conférer une publicité maximale à la vente publique afin de réunir le plus grand nombre d'enchérisseurs. En revanche, elle accueille sa demande à l'encontre de Google, enjoignant à Google Spain et Google Inc. de retirer les données à caractère personnel le concernant de son index ainsi que d'empêcher l'accès à celles-ci à l'avenir. Google refuse d'obtempérer et forme un recours en annulation contre cette décision de l'autorité espagnole. C'est dans le cadre de ce recours que la Cour de Justice a été saisie de plusieurs questions préjudicielles concernant l'interprétation de plusieurs dispositions de la directive européenne du 24 octobre 1995 sur la protection des données à caractère personnel.

Plusieurs enseignements découlent de la décision du 13 mai 2014. Tout d'abord, l'activité de moteur de recherche réalise un « traitement de données à caractère personnel »au sens de la directive. La collecte des informations publiées sur Internet par des tiers, l'indexation de manière automatique, le stockage temporaire et la mise à disposition des internautes selon un ordre de préférence caractérise bien un traitement de données à caractère personnel. Ensuite et surtout, la

---

18 TGI Paris, ord. réf., 15 février 2012

19 TGI Paris, 6 novembre 2013

20 En cela le passage, dans la dernière mouture du projet de Règlement, du droit à l'oubli au droit à l'effacement est heureux. L'oubli est définitif, l'effacement provisoire. Il est préférable que notre droit s'en tienne à cet effacement provisoire (l'oubli étant impossible à assurer sur l'Internet).

21 CJUE, gde ch., 13 mai 2014, aff. C-131/12, Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos e.a. : JurisData n° 2014-009597 ; JCP E 2014, 1326, note M. Griguer ; JCP E 2014, 1327, note G. Busseuil. Comm. Com.electr 2014 Etude 13 A. Debet

Cour de justice juge que le moteur de recherche doit mettre en œuvre les droits de rectification, d'effacement des données et le droit d'opposition à un traitement lorsque les données traitées ne sont plus adéquates ou pertinentes et excessives par rapport aux finalités. Un tel traitement de données est en effet« susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel lorsque la recherche à l'aide de ce moteur est effectuée à partir du nom d'une personne physique dès lors que ledit traitement permet à tout internaute d'obtenir par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet, qui touchent potentiellement à une multitude d'aspects de sa vie privée et qui, sans ledit moteur de recherche, n'auraient pas ou seulement que très difficilement pu être interconnectées, et ainsi d'établir un profil plus ou moins détaillé de celle-ci ». Dès lors, si les conditions prévues par la directive sont effectivement satisfaites, l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne. C'est donc ici le droit au respect de la vie privée et le droit de maîtrise des données personnelles protégés par les articles 7 et 8 de la Chartes des droits fondamentaux qui justifie l'existence de ce droit d'effacement. « Ces droits qui prévalent (...) non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne » ne sont pas toutefois absolus. La Cour émet en effet une importante réserve puisqu'elle considère que « s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question », alors cette prérogative d'effacement devrait être paralysée. Le juge, ici, comme à l'occasion de la friction d'autres droits fondamentaux' s'efforce de parvenir à un équilibre. Pour cela, il utilise le principe de proportionnalité ou celui de finalité. L'on notera pour finir que l'exercice de ce droit n'est nullement conditionné à l'existence d'un préjudice. Avant même l'adoption du Règlement données personnelles, la Cour de justice consacre donc ce droit d'effacement des données personnelles que l'on qualifie hâtivement de droit à l'oubli. Google a rapidement réagi à cette condamnation en instituant un formulaire de droit de suppression des données personnelles dont la mise en œuvre s'avèrera délicate[22].

Une analyse rigoureuse montre donc bien que l'objet du droit à l'oubli est réduit. Qu'en est-il de la nature de ce « droit » ?

II- Une nature imprécise

22 Sous réserve de prouver son identité et d'identifier le lien litigieux aux services de Google, il est en effet désormais possible de faire effacer les résultats de recherche qui incluent notre nom et qui seraient « inadéquats, pas ou plus pertinents ou excessifs au regard des finalités du traitement ». (A. Fournier « Google lance son formulaire oubli pour les Européens », Le Monde 30 mai 2014) L'appréciation s'avère fort difficile pour Google (au demeurant, peut-on être « juge » et « partie » ?). De très nombreuses demandes vont être formulées (A. Fournier « Les internautes se précipitent sur le formulaire oubli de Google », Le Monde 3 juin 2014). Dans quel délai vont-elles êtres traitées ? Faut-il au préalable saisir l'éditeur ?

11. « Droit à » vous avez dit « Droit à » ? Le droit à l'oubli, à l'examen, présente une nature bien imprécise. Contrairement à ce que l'expression du « droit à » laisse penser, nous ne sommes pas en effet en présence d'un droit subjectif. Il suffit, pour s'en convaincre, de considérer aussi bien le droit à l'oubli, général, que le droit à l'oubli numérique particulier.

12. Droit à l'oubli ou devoir de réserves ? L'exemple du passé judiciaire. De nombreux diffuseurs (chaines de télévision, journaux papiers ou électroniques…) puisent aujourd'hui abondamment dans le passé judiciaire criminel de certains individus afin de réaliser des documentaires ou des articles dont le public est friand. C'est dans ce contexte que « le droit à l'oubli » général a pu être (et est toujours) mis en avant. Nous avons ici démontré[23] en nous appuyant sur la jurisprudence française et européenne (Cour européenne des droits de l'homme mais aussi décisions de cours européennes), qu'en réalité ce « droit à l'oubli » n'existe pas en tant que tel. Il existe en revanche un devoir de ne pas faire resurgir le passé judiciaire d'un individu sans respecter un certain nombre de conditions : caractère historique des faits diffusés, intérêt à la resocialisation des personnes condamnées, degré d'exposition de la personne… Or, comme nous l'avons souligné : « Le fait de rappeler à certains journalistes certaines règles de comportement, de loyauté, ne revient pas à consacrer au profit des personnes victimes de ces mauvais usages, un nouveau « droit à »[24].

13. Droit à l'oubli. Droit subjectif et Droit objectif. Le « droit à » l'oubli numérique présente la même ambiguïté. Le droit positif de la loi informatique fichiers et libertés ou le droit prospectif du projet de Règlement données personnelles consacrent le droit d'opposition, le droit d'exiger le respect de la finalité du traitement ou de la durée de conservation des données. Or tous ces droits représentent des prérogatives conférées par le droit objectif. C'est bien en effet la « loi » qui détermine les conditions du droit d'opposition ou la durée de conservation des données[25]. L'on ne peut donc parler ici de droit subjectif. Seul le droit de retirer « son consentement sur lequel est fondé le traitement » peut donc se rattacher à un droit subjectif encore qu'il faille certainement examiner les conditions dans lesquelles ce retrait (généralement à la suite des sollicitations commerciales d'un opérateur du commerce électronique) pourra s'exercer[26].

---

23 J.-M Bruguière et B. Gleize, « Les droits de la personnalité », Ellipses à paraître

24 J.-M Bruguière, Dans la famille des droits de la personnalité, je voudrais… D. 2011 n°1 p. 28

25 Une semblable conclusion doit être portée à l'égard des « nouveaux » cas d'effacement prévus par le projet de Règlement données personnelles. L'oubli peut être demandé en présence de données traitées de façon illégale ou lorsque qu'une décision de l'autorité judiciaire ou administrative l'ordonne. C'est toujours la loi qui structure ce droit.

26 Ce droit de retrait fera (fait) en effet souvent l'objet de renonciation de la part de l'internaute en contrepartie de quelque chose : un accès à des services particuliers par exemple. Il faut surtout bien comprendre le sens de ce retrait. Plutôt que de consacrer un irréaliste droit de propriété de l'internaute sur ses données personnelles (sur ce vieux débat Y. Pouillet « Le fondement du droit à la protection des données nominatives : propriétés ou libertés » in « Nouvelles technologies et propriété » Litec 1992), ce mécanisme révèle la volonté de mettre le cyberconsommateur à l'écart d'une trop forte pression promotionnelle. Le droit de retrait est le droit de se retirer de l'espace marchand dans l'économie numérique. Un droit en quelque sorte de seconde ou plutôt troisième génération des droits de l'homme, droit à ne pas subir de « pollution » publicitaire suite à la captation de données personnelles (d'où la reconnaissance du retrait). Ou alors plus simplement, droit de circuler librement sur l'Internet.

Le droit à l'oubli est donc un droit inconsistant. Il ne doit pas être condamné pour autant. Ce droit présente en effet un intérêt, non pas pour ce qu'il est, mais pour ce qu'il révèle : un manque dans notre système juridique c'est-à-dire l'absence d'un droit de maîtrise des informations personnelles.

Section 2- Le droit au respect de ses informations personnelles : un droit à consacrer

Le droit à l'oubli cache selon nous un autre droit : le droit au respect de ses informations personnelles. Après avoir montré que ce droit existe (I), il conviendra de saisir son essence (II).

I- L'existence du droit

Le droit sur les informations personnelles est avant tout une construction doctrinale qui a reçu de nombreuses consécrations jurisprudentielles et législatives.

14. Droit sur les informations personnelles. Proposition doctrinale. Daniel Gutman fut l'un des premiers à proposer ce droit de contrôle sur les informations personnelles[27] sans considération particulière, au moment de l'énoncé de sa thèse, du sort ces traces numériques. Pour l'auteur, la vie privée n'est qu'un ensemble d'informations présentant un caractère personnel. La vie privée ne doit plus être perçue comme un ensemble d'actes auxquels la personne doit se livrer librement (auquel cas la vie privée ne se distinguerait pas de la liberté individuelle). La vie privée est avant tout un ensemble de données dont la connaissance ou l'ignorance par les tiers est l'enjeu fondamental[28]. Cette proposition est intéressante. Elle permet tout d'abord de dépasser le cadre restreint de la vie privée comme cela a été fait en droit du travail par exemple. Nous savons que le juge social a su faire émerger une notion de vie personnelle du salarié aux côtés de celle de vie privée[29]. Elle favorise ensuite l'appréhension de simples données identifiantes, ce qui n'est pas toujours facile pour le juge civil. L'on a ainsi coutume de dire que la vie privée englobe l'adresse. Or à l'analyse, cette position n'est pas tout à fait exacte. C'est parce que l'information est personnelle, c'est-à-dire identifiante, que la protection est assurée. La thèse de Daniel Gutman semble donc tout à fait opportune.

15. Objections. Elle se heurte toutefois à plusieurs objections. Une telle proposition réduirait à néant toute la construction prétorienne autour de l'article 9 du Code civil. La savante élaboration des contours de la vie privée par le juge disparaitrait au profit d'une notion d'information personnelle beaucoup trop englobante. Il y a en effet une facilité de langage à évoquer l'information personnelle. L'information personnelle n'est pas toujours la donnée personnelle de la loi informatique fichiers et libertés[30] et la donnée personnelle ne coïncide pas,

---

27 Daniel Gutmann, Le sentiment d'identité, LGDJ, Coll. Bibl. dr. privé, 2000, t. 327

28 Op. cit. n°261

29 Philippe Waquet, Vie professionnelle et vie personnelle du salarié, Cahiers Sociaux du Barreau de Paris, 1994, p. 289.

30 Sur ces distinctions cf. Sur ces deux termes, v. Pierre Catala, Le marché de l'information (aspects juridiques), article paru en 1995 et reproduit in Le droit à l'épreuve du numérique. Jus ex Machina, PUF, 1998, p. 323 s., spéc. p. 324

comme nous l'avons souligné, avec la vie privée. La donnée personnelle recoupe elle-même plusieurs réalités. Les sociologues opposent les données dites « déclaratives » (qui sont livrées par l'internaute lui même : le pseudo, le mot de passe...) et les données « agissantes » (qui sont générées par l'internaute au cours de son activité sans réelle conscience de sa part)[31]. Certains juristes ont pu proposer de distinguer les données personnelles aux données de communications électroniques (données d'identification, de connexion, de trafic, de consultations....)[32]. Ces propositions doctrinales ont reçu un certain écho législatif. La loi du 21 juin 2004 sur la «confiance dans l'économie numérique » dessine ainsi, à la charge des opérateurs de communications électroniques, un régime particulier de conservation des «données de communications » pour identifier notamment les personnes qui ont créé un contenu en ligne. L'information personnelle ne peut donc raisonnablement englober l'information sur la vie privée, les données personnelles, les données de communication électroniques.

16. Droit sur les informations personnelles. Droit positif. Chartes des droits fondamentaux. Cour constitutionnelle allemande, loi informatique fichiers et libertés. L'information personnelle doit donc être consacrée pour elle-même sans confusion possible avec le droit au respect de la vie privée. Ceci est déjà le cas en Europe avec la Chartes des droits fondamentaux. Dans la Chartes, le droit au respect de la vie privée (article 7) précède en effet le droit à la protection des données personnelles (article 8)[33]. C'est surtout la décision de la Cour constitutionnelle Allemande du 1983, sur laquelle nous reviendrons plus bas, qui doit servir de base à ce droit de contrôle des informations personnelles[34]. A l'occasion de l'examen d'une loi sur le recensement, sur le fondement du respect de la dignité humaine (article 1 er de la Constitution) et du droit au développement de la personnalité (article 2) la Cour souligne qu'il est nécessaire « pour un développement libre de la personnalité que dans les conditions modernes de traitement des données l'individu ait une protection contre la collecte, la conservation et la transmission illimitées de ses données à caractère personnel ». En France, la loi informatique, fichiers et libertés est une des manifestations les plus éclatantes (peut-être même l'une des premières) de ce droit sur les informations personnelles ; la personne se voyant reconnaître différentes prérogatives : droit d'opposition, droit d'accès, droit de rectification .... Ce droit n'est en rien un droit absolu comme cela est, une nouvelle fois, fort bien mis en valeur par la Cour constitutionnelle allemande. « L'individu ne possède pas un droit qui lui permettrait d'avoir une

---

31 F. Georges Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0, Réseaux 2009 n°154 p. 165

32 M. Vivant (ss. dir.) Lamy droit de l'informatique et des réseaux 2011 n°555 qui isole dans les « données personnelles » les « données de communication électronique ».

33 Cette perspective n'est pas toujours adoptée. Dans la Convention 108 du Conseil de l'Europe, par exemple, la protection des données personnelles est fondue dans la protection de la vie privée. Selon l'article 1 er : « Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données») ».

34 Sur cette décision, cf. Y. Pouillet et A. Rouvroy, Le droit à l'autodétermination informationelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie in Etat de droit et virtualité .Montréal Thémis 2009 p. 159.

maîtrise absolue, illimitée de ses données ; sa personnalité dépend en réalité de la communication qui se développe au sein de la communauté sociale. L'information, même liée à la personnalité, est le reflet d'une réalité sociale et ne peut être associé uniquement à l'individu concerné ». L'information personnelle n'est donc pas la propriété de l'individu. Sa maîtrise a vocation à être assuré par le principe de finalité et une gestion fiduciaire[35].

II- L'essence du droit

17. Les difficultés de rattachement du droit. L'existence de ce droit sur les informations personnelles reconnue, il reste à saisir son essence. Plus précisément se pose la question de savoir à quoi rattacher cette nouvelle prérogative : le droit au respect de la vie privée, la loi informatique fichier et libertés, seule, un droit au respect de sa personnalité sociale ... ? L'essence de ce droit ne peut en effet être perçue qu'au travers de cette délicate question du rattachement. Nous allons nous efforcer de démontrer que seul un droit au respect de la vie privée, élargi, est à même de rendre compte de cette nouvelle prérogative. Un manque que révèle très certainement ce droit à l'oubli.

18. La loi informatique, fichiers et libertés dans le Code civil. Un auteur, Judith Rochfeld, a pu récemment proposer d'importer aux côtés de l'article 9 du Code civil les dispositions principales de la loi informatique fichiers et libertés[36]. Cette recodification du droit des personnes ne vise pas ici à fondre la vie privée dans le droit des données personnelles mais à faire cohabiter les deux législations ce qui est bien différent. Formellement cette position a été consacrée dans la Chartes des droits fondamentaux, comme nous venons de le voir. Dans le fond, cette proposition, sans entrainer le bouleversement majeur de la thèse de Daniel Gutman, permettrait une fertilisation réciproque du droit au respect de la vie privée et du droit des données personnelles. Elle se heurte toutefois elle aussi à plusieurs critiques. L'on ne sait pas pourquoi le Code civil, plus que tout autre code, devrait accueillir cette loi informatique fichiers et libertés. A accepter le principe de cette recodification, nous pensons que le Code de la consommation serait tout aussi légitime pour accueillir cette législation. Les difficultés pratiques se posent aujourd'hui pour des données personnelles collectées sur l'Internet dans des relations de professionnels à consommateurs (que l'on songe aux données collectées sur les réseaux sociaux). Le rapprochement de la loi informatique, fichiers et libertés de l'article 9 du Code civil pourrait également favoriser le mouvement de patrimonialisation de certains droits de la personnalité. Les internautes seraient ainsi tentés de commercialiser leurs données personnelles, comme le font aujourd'hui certains titulaires du droit à l'image ou droit sur la voix. Enfin, il faut

---

35 J.-M Bruguière, Les données publiques et le droit, op. cit. n°100. « Les données publiques » (mais le propos vaut également pour les données personnelles) « peuvent être appréhendées en tant que patrimoine d'affectation. Cette thèse rejoint de nombreuses positions de la CNIL lorsqu'elle est amenée à se prononcer sur les pratiques de détournement de finalité de certains traitements. Loin de s'interroger sur l'aptitude du maitre du traitement à recevoir certains droits sur l'information, la Commission s'attache avant tout à faire respecter, à travers certains paramètres (le contenu informatif d'une base, la mission de l'organisme, les destinataires de l'information..) l'affectation d'une richesse informationnelle à certaines utilités ».

36 J. Rochfeld, article précité

bien voir que la protection de la vie privée est avant tout individuelle et celle des données personnelles, collective comme cela a été fort bien relevé[37].

19. Proposition de reconnaissance d'un droit de contrôle des informations personnelles dans le cadre d'un droit au respect de la personnalité sociale dans le Code civil. Sans vouloir nécessairement nous singulariser, nous pensons que le droit sur les informations personnelles pourrait trouver sa place aux côtés du droit au respect de la vie privé ou du droit à l'image dans l'ensemble plus large du droit au respect de la personnalité sociale. Il servirait ainsi de porte parole à l'inconsistant « droit à l'oubli » aujourd'hui proposé. Expliquons-nous. Le droit de contrôle des informations personnelles entretient des liens étroits avec le développement de la personnalité sociale comme l'a souligné la Cour constitutionnelle allemande. «Si l'individu ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est limitée ». Ce droit de contrôle des informations personnelles qui concourt ainsi au développement de la personnalité n'a pas besoin d'être consacré tel quel dans le Code civil. Nul n'est besoin de décliner à la suite de l'article 9 du Code civil les : « Chacun a droit au respect de son image », « Chacun a droit au respect de ses informations personnelles »... En revanche, il serait utile de reformuler l'article 9 du Code civil en s'inspirant des travaux de la Commission de révision du Code civil de 1951 (art. 165) : « Chacun a droit au respect de sa personnalité ».Cette proposition rejoindrait celle faite par Jacques Mestre il y a quelques années[38]. Comme le souligne l'éminent auteur, il serait utile de consacrer « un nouveau droit de la personnalité, consistant dans celui, reconnu à toute personne physique et à toute personne morale, à ce que sa personnalité ne soit pas l'objet d'une altération publique ». Plus précisément, la consécration ne serait pas celle d'un « nouveau droit de la personnalité » mais plutôt celle d'un nouveau Droit, des droits de la personnalité; le droit au respect de la personnalité les englobant tous. La formulation de l'article 9 du Code civil pourrait-être plus précisément la suivante: « Chacun a droit au respect de sa personnalité sociale ». Notre droit n'a pas vocation à protéger la personnalité elle-même (cela incombe à la psychologie). Seule la personnalité sociale doit retenir l'attention. C'est en effet la personnalité de l'individu qui se développe en société qui mérite protection. Le droit au respect de sa personnalité sociale aurait vocation à intégrer tous les droits de la personnalité : droit au respect de la vie privée, droit à l'image, droit à l'honneur, droit au respect des informations personnelles, droit aux secrets, droit au nom. L'économie d'écriture serait ainsi assurée pour le législateur. Ce droit bénéficierait à toutes les personnes, physiques, comme morales ; la notion de vie privée s'adressant plutôt aux personnes physiques[39]. Le contenu de chacun de ces droits n'en

---

37 G. Loiseau, « Les métamorphoses de la protection de la vie privée à l'heure du numérique », Légipresse n°284 p. 345. Sur cette discussion, « Reste que sans déposséder l'individu de son pouvoir propre, l'action de la CNIL pourvoit à une défense collective de la vie privée contre ce qui représente en réalité un risque d'atteinte individuelle à celle-ci ».

38 J. Mestre, La protection indépendante du droit de réponse, des personnes physiques et des personnes morales contre l'altération de leur personnalité aux yeux du public JCP 1974, I, 2623,

39 Certaines décisions ont pu juger du contraire. La cour d'appel d'Aix en Provence a ainsi souligné (Aix-en-Provence, 10 mai 2001, D. 2002. Somm. 2299, obs. A. Lepage) avec audace « que les personnes morales sont

serait pas modifié. Tout au plus le juge devrait établir un lien entre le droit au respect de la personnalité sociale et chacun des droits de la personnalité, ce qui ne semble pas trop difficile si l'on considère certaines décisions de la Cour de cassation[40]. Le Conseil constitutionnel français, tout comme la Cour constitutionnelle allemande, devrait imaginer un point d'ancrage fondamental à ce droit à la personnalité sociale. Mais là encore, l'exercice ne semble pas hors de portée[41]. L'envahissant « droit à » l'oubli pourrait ainsi utilement être rattaché au droit au respect des informations personnelles et fondu dans ce droit à la personnalité sociale. Si le droit est la

---

susceptibles de subir une atteinte à leur vie privée dès lors qu'elles sont titulaires de droits, non pas identiques, mais analogues aux droits de la personnalité tels que le droit au nom, le droit au secret de leur vie intérieure parallèlement à la vie publique qui justifie leur existence en raison de leur objet ». En faveur de la reconnaissance des droits de la personnalité pour les personnes morales, H. Martron, Les droits de la personnalité des personnes morales de droit privé, LGDJ 2011, Préf. J.-C Hallouin et J.-M Bruguière et B. Gleize, Droits de la personnalité, Ellipses, à paraître. A noter d'ailleurs que le projet de Règlement des données personnelles est réservé aux personnes physiques et à elles seules (cf article 1 er).

40 Ainsi dans un arrêt important, dans le cadre du droit au respect de la vie privée, la Cour de cassation n'a pas hésité à protéger la personne contre l'altération de sa personnalité au cas dans lequel les traits faux qui étaient prêtés ne procédaient pas d'une erreur mais étaient le fruit de l'imagination au service d'une création littéraire. La Cour juge qu'« une œuvre de fiction, appuyée en l'occurrence sur des faits réels, si elle utilise des éléments de l'existence d'autrui, ne peut leur en adjoindre d'autres qui, fussent-ils imaginaires, portent atteinte au respect dû à sa vie privée » (Civ. 1re, 7 févr. 2006, n° 04-10.941, JCP 2006. II. 10041, note G. Loiseau, RCA 2006. 107, RTD civ. 2006. 279, obs. J. Hauser). Est ainsi étendu de façon importante le champ d'application de l'article 9 du code civil. Il ne s'agit plus seulement en effet de protéger la personne contre les révélations faites sur sa vie privée. Il s'agit d'éviter de donner à penser aux tiers que la personne présente tel ou tel trait qui ne correspond pas à la réalité. Cette solution a été récemment confirmée dans un arrêt de la Cour de cassation du 20 mars 2014 (à propos de l'imitation de la voix d'une petite fille d'un célèbre homme politique). Cass. civ.. 1ère, 20 mars 2014, n° 13-16.829, JurisData n° 2014-005207, Com.com.électr. 2014 n°6 comm. 55 A.Lepage. Légipresse 2014 n°317 p. 352 note G. Lécuyer. La Cour de cassation ne s'attache pas ici à l'imitation de la voix en tant qu'elle constituerait l'atteinte à la personnalité par la création d'une confusion. Elle ne retient pas plus l'existence de révélations intempestives qui, dévoilant ses relations avec son grand-père, porteraient atteinte au droit au respect de la vie privée de l'enfant. De façon bien différente, la Cour de cassation considère que le droit a été atteint parce que «de droit au respect de sa vie privée et familiale s'oppose à ce que l'animateur d'une émission radiophonique, même à dessein satirique, utilise la personne de l'enfant et exploite sa filiation pour lui faire tenir des propos imaginaires et caricaturaux à l'encontre de son grand-père ou de sa mère, fussent-ils l'un et l'autre des personnalités notoires et dès lors légitimement exposées à la libre critique et à la caricature incisive ». L'on retrouve le droit pour la petite fille de s'opposer à l'altération de sa personnalité sociale. Guillaume Lécuyer observe ainsi très justement : « Ce faisant, la première chambre civile élude la question de savoir où se situe la frontière entre la vie privée et la vie publique. Elle privilégie une conception essentialiste de la vie privée. Dans cette optique, cette valeur protégée doit permettre aux individus de construire leur vie comme ils l'entendent, sans interférence provenant des regards d'autrui. La vue privée idéale est celle au cours de laquelle l'individu peut faire ses choix de vie en toute indépendance et définir sa personnalité sans être gêné ou freiné par des ingérences extérieures ».

41 Le Conseil constitutionnel dans sa décision du 23 juillet 1999 (n°99-416 DC J● 28 juillet 1999) considère que la liberté personnelle de l'article 2 de la Déclaration des droits de l'homme implique le respect de la vie privée. Il est dès lors aisé de considérer que cette liberté personnelle intègre également le respect de la personnalité sociale. Autrement dit la liberté de l'article 2 pourrait être aussi un porte parole du développement de la personnalité.

plus puissante école de l'imagination[42], il ne faut pas que cette imagination déréglée conduise à l'élaboration des droits fantômes[43].

42 Selon la célèbre formule de Jean Giroudoux, La Guerre de Troie n'aura pas lieu, 1935

43 L'on se souvient peut être que Roubier écrivait ainsi dans la préface de la thèse de Roger Nerson que cette catégorie des droits de la personnalité était une des « théories les plus absurdes du droit civil », dans laquelle il ne voyait que « des droits fantômes conçus par des imaginations déréglées ».

CHAPITRE 3

Droit à l'oubli des personnes condamnées versus liberté d'expression : un combat perdu d'avance ?[1]

1. La revendication d'un droit à l'oubli est protéiforme et diffuse : si elle concerne à l'heure actuelle de manière significative l'outil numérique, cette demande sociale ne se réduit pas à ce seul champ. Cet éventuel droit est brandi à l'encontre de la liberté d'expression, quel que soit le support de celle-ci. Ainsi, face à la liberté de création littéraire, cinématographique[2] ou face à la liberté de la presse et au droit à l'information (pour la presse écrite[3], audiovisuelle comme pour internet[4]), le droit à l'oubli est envisagé le plus souvent comme un corollaire du droit à la vie privée. Cette confrontation entre droit à l'oubli et liberté d'expression est ancienne et a fourni matière à des développements contentieux conséquents. Est ainsi invoqué le droit des individus à s'opposer « à la reprise sans leur consentement d'informations qui dans leur temps furent licitement révélées au public mais dont l'actualité ne justifie pas la diffusion »[5], en particulier lorsque ces informations sont exploitées par un média audiovisuel.

2. La mode des documentaires-fictions, avec force reconstitutions des faits et dramatisation, ou d'autres émissions explorant le passé judiciaire d'anciens condamnés, conduit à

---

1 par Hafida Belrhali-Bernard, Professeure à la faculté de droit de Grenoble

2 A propos d'une fiction reprenant fidèlement les circonstances d'un drame particulièrement atroce et par ailleurs ancien, la Cour d'appel de Versailles souligne que ce film « constitue une immixtion dans le for intérieur de X... pour s'analyser en un rappel de faits et situations irrésistibles profondément et irrémédiablement traumatisants ». CA Versailles, 14 novembre 2002, D. 2003, p. 1715, note C. Caron. En l'espèce, selon C. Caron, lorsque la divulgation des évènements les a fait, en quelque sorte, tomber dans le domaine public, l'écoulement du temps plutôt que de provoquer une érosion des droits de la personnalité au profit de la liberté d'expression de l'auteur conduit exceptionnellement à ramener ces faits dans le giron de la vie privée. La justification d'une telle solution serait précisément le droit à l'oubli. C. Caron, A propos du conflit entre les œuvres de fiction et la vie privée, D. 2003, p. 1715.

3 Le droit à l'oubli d'anciens condamnés fait également débat lorsque la presse diffuse les photographies de personnes condamnées par le passé et ayant eu des liens avec une personne récemment appréhendée. Voir par exemple le cas de Florence Rey, l'affaire Rey-Maupin datant de 1994. Cette affaire fut de nouveau évoquée en 2013 et des photographies de l'intéressée de nouveau diffusées alors que celle-ci a été libérée en 2009 après 15 années de détention. Cette rediffusion est liée à un élément d'actualité : l'arrestation d'Abdelhakim Dekhar, après les attaques des sièges de BFM-TV et de Libération à la Défense, qui lui aussi avait été condamné en 1994 lors de la précédente affaire (V. Le Monde, 24 novembre 2013).

4 V. A. Marais, Le droit à l'oubli numérique in B. Teyssié (dir.), La communication numérique, un droit, des droits, Ed. Panthéon-Assas, 2012, p. 63 s. Quant aux difficultés soulevées par la mémoire de l'outil numérique pour les informations d'ordre judiciaire, on renverra à l'introduction de la contribution de F. Girard, Sens et possibilités d'un « droit à l'oubli » aux Etats-Unis, p. 150 s. Par ailleurs, après la remise de notre rapport, la Cour de justice de l'Union européenne a rendu la fameuse décision consacrant un droit à l'oubli numérique relative à Google, v. CJUE, gr. ch., 13 mai 2014, aff. C-131/12, Google Spain SL et a., comm. G. Busseuil, JCP E., 2014, n°24, comm. 1327.

5 A. Lepage, Droit à l'oubli, une jurisprudence tâtonnante, D. 2001, p. 2079.

remettre sur le devant de la scène des évènements passés que ces protagonistes préfèreraient ne pas voir rappelés. La confrontation entre droit à l'oubli et liberté d'expression surgit ainsi de manière récente dans le champ audiovisuel. La revendication de ce droit apparaît là de manière autonome au sens où il s'agit bien d'invoquer le seul écoulement du temps comme nécessitant un oubli : celui-ci constituerait un droit subjectif des individus à opposer aux journalistes et sociétés de production de ces émissions. Toutefois, pour paraphraser la formule de P. Poncela, les liaisons du droit à l'oubli et de la liberté d'expression sont bien des liaisons dangereuses[6]. La cause des anciens condamnés revendiquant un droit à l'oubli de leur passé judiciaire semble entendue : face à la puissante liberté d'expression, ancrée dans les textes et la jurisprudence, le droit à l'oubli, revendiqué par des acteurs sociaux mais non consacré par le droit positif, semble bien démuni.

3. Un jugement récent du Tribunal de grande instance de Paris, en date du 14 janvier 2013[7], fournit une illustration contentieuse de ce combat inégal. Il permet d'appréhender les différentes dimensions de cette confrontation. En l'espèce, un numéro de l'émission *Enquêtes criminelles* diffusée sur la chaîne M6 et produite par la société CAPA Presse a retracé l'affaire dite des « paras de Francazal ». Ces quatre parachutistes de la base de Toulouse-Francazal ont été condamnés en 1991 à la réclusion criminelle à perpétuité pour viols et meurtres avec actes de barbarie. L'un d'entre eux, incarcéré depuis plus de 21 ans, agit notamment contre la société

---

6 P. Poncela, Les liaisons dangereuses du droit à l'image et du droit à l'information du public, Chronique de l'exécution des peines, RSC juillet/septembre 2012, p. 649 s.

7 17ème ch., 11/03875, Légipresse 2013, n° 303, I, p. 137. Après la remise de notre rapport, d'autres décisions sont intervenues que nous mentionnons ici. A propos du docu-fiction, Virée criminelle, la Cour d'appel de Paris a adopté une solution conforme à la jurisprudence antérieure en précisant que : « les faits criminels, leur contexte, et la personnalité du demandeur ont été licitement révélés au public par les comptes rendus judiciaires ; qu'en droit, la relation de faits publics déjà divulgués ne peut constituer en elle-même une atteinte au respect dû à la vie privée ». La cour précise par ailleurs que le « droit à l'oubli, contrairement à ce que soutient le demandeur, n'a aucune reconnaissance légale et ne saurait prévaloir sur le droit du public à l'information exhaustive et objective » (CA Paris, pôle 2, 7e ch., 26 févr. 2014, n° 13/01241, T. E. B. et a. c/ SA Capa Presse et a., inédit). En revanche, dans l'affaire Intime conviction, le juge des référés du Tribunal de grande instance de Paris puis cette même cour d'appel ont adopté et confirmé une position remarquée d'interdiction de diffusion, qui a semblé se distinguer des solutions précédentes. En l'espèce, il est précisé que « même en admettant que M. Muller ait lui-même exposé dans les médias des éléments de sa vie privée, ces révélations antérieures ne sont pas de nature à en justifier de nouveau la divulgation sans l'accord de l'intéressé » (TGI Paris, réf., 27 févr. 2014, n° 14/51822. – CA Paris, pôle 1, 2e ch., 28 févr. 2014, n° 14/04355, SAS Maha Productions c/ J.-L. M. : JurisData n° 2014-003374 ; JCP G 2014, 295, obs. E. Derieux ; RLDI mars 2014, n° 3393). Ces décisions, particulièrement protectrices du droit à la vie privée de l'intéressé, concernent un programme de la chaîne Arte inspiré par l'affaire du Dr Muller, acquitté du meurtre de son épouse. Il s'agissait non seulement d'un téléfilm mais également de « webvidéos » permettant aux internautes d'assister à un procès d'assises fictif et de se prononcer pour l'un ou l'autre des verdicts envisagés. La cour souligne que « même si une partie des faits tenant à la vie privée de M. Muller ont été divulgués par la presse lors de sa comparution devant la cour d'assises, ils ne peuvent cependant être licitement repris dès lors que le programme Intime conviction est une œuvre de fiction, et non pas un documentaire ou un article d'information ». La cour insiste sur les caractères de l'œuvre qui, inspirée de faits réels, y mêle des éléments fictifs et précise que « la création audiovisuelle peut certes s'inspirer de faits réels et mettre en scène des personnages vivants mais qu'elle ne saurait, sans l'accord de ceux-ci, empiéter sur le terrain de leur vie privée dès lors que l'œuvre ainsi réalisée ne présente pas clairement les éléments ressortant de celles-ci comme totalement fictifs ». Il conviendra donc d'observer les éventuels prolongements de cette jurisprudence. Pour autant, ces décisions ne consacrent pas de droit à l'oubli et intéressent particulièrement les rapports entre fiction et vie privée. B. Montels, Un an de droit de l'audiovisuel, Communication Commerce électronique, n°6, 2014, chron. 6, n°21.

productrice en invoquant le respect de son droit à la vie privée et de son droit à l'image et demande à la juridiction de retenir à son profit un droit à l'oubli. Il réclame à la fois la réparation de son préjudice moral et l'interdiction de rediffusion de l'émission ou, subsidiairement, son anonymisation. Rejetant la requête, le Tribunal de grande instance de Paris a considéré que l'atteinte à la vie privée et au droit à l'image n'était pas constituée et que « le droit à l'oubli, qui n'est consacré par aucun texte, ne peut, en l'espèce, prévaloir « sur le droit du public à une information libre, complète et objective sur une affaire pénale ». Le même tribunal avait précédemment rejeté la demande en référé de l'intéressé réclamant l'interdiction de la diffusion éminente de l'émission[8]. Ce jugement confirme les termes d'une jurisprudence traditionnelle sur la balance des intérêts en présence (1). Il comporte par ailleurs une dimension plus originale en réfutant un raisonnement relatif aux droits spécifiques des détenus consacrés par la loi pénitentiaire de 2009 (2). Il démontre qu'au total la revendication formulée par les personnes condamnées ne reçoit pas un écho favorable en l'état actuel du droit. Ce constat justifie de formuler des propositions relevant de la *soft law*. Dans ce domaine comme en matière numérique, si le droit à l'oubli n'est pas inscrit dans le marbre de la loi, il peut en revanche prospérer utilement dans le cadre de chartes ou de règles de déontologie (3).

Section 1- Droit à l'oubli *versus* liberté d'expression : la balance des intérêts en présence

4. Une fois n'est pas coutume, la jurisprudence de la Cour européenne des droits de l'homme sur notre sujet n'a qu'un faible intérêt. La CEDH a certes jugé que des « informations, une fois portées à la connaissance du public par l'intéressé lui-même, cessent d'être secrètes et deviennent librement disponibles »[9]. Elle a par ailleurs prêté attention aux effets de l'écoulement du temps pour reconnaître qu'une restriction de la liberté d'expression, autrefois justifiée, n'a plus lieu d'être[10]. Elle considère également que, « lorsqu'il s'agit d'événements qui s'inscrivent dans l'Histoire ou relèvent de la science, il peut au contraire sembler qu'au fil du temps, le débat se nourrit de nouvelles données susceptibles de permettre une meilleure compréhension de la réalité des choses ». Elle valorise ainsi le droit à l'information, le temps passant[11]. En revanche, cette jurisprudence n'a pas, à notre connaissance, apporté sa contribution à l'émergence d'un véritable droit à l'oubli face à la liberté d'expression. La confrontation des deux droits reste donc tranchée, pour le sujet qui nous intéresse, par la juridiction judiciaire dont la jurisprudence mérite d'être analysée (I) Le conflit entre ces droits a de plus été éclairé, au-delà de notre sujet à proprement parler, par une jurisprudence constitutionnelle récente (II).

I- La confrontation du droit à l'oubli des personnes condamnées et de la liberté d'expression dans la jurisprudence judiciaire

---

8 Ordonnance du 16 août 2010, n°10-56840.

9 CEDH, 5e sect., 23 juill. 2009, Hachette Filipacchi Associés (Ici Paris) c/ France, req. n° 12268C/03, § 52 : Légipresse 2009, III, p. 179, note L. Marino

10 V. CEDH, 18 mai 2004, Éditions Plon c/ France, n° 58148/00, D. 2005, p. 1838, note A. Guedj, D. 2005, somm. p. 2539, obs. N. Fricéro, RTD civ. 2004, p. 483, obs. J. Hauser.

11 CEDH, 7 nov. 2006, n° 12697/03, Mamère c/ France, D. 2007, jurispr. p. 1704, note J.-P. Marguénaud.

5. La jurisprudence relative au droit à l'oubli et à la liberté d'expression a connu des inflexions qu'il convient de rappeler de manière synthétique. Si les solutions adoptées ne sont pas nécessairement favorables aux demandeurs, surtout dans la période récente, certains jugements et arrêts soulignent néanmoins la légitimité de la revendication d'un droit à l'oubli[12]. Cette jurisprudence a pour intérêt d'expliciter les termes d'un débat à propos d'un droit qui, il faut la rappeler, n'est pas reconnu textuellement ni en termes généraux, ni au profit des seules personnes condamnées.

6. La jurisprudence judiciaire[13] sur le sujet est traditionnellement présentée en fonction du repère que constitue l'arrêt de référence de la Cour de cassation du 20 novembre 1990. Avant 1990, diverses décisions de juridictions du fond favorables au droit à l'oubli ont été rendues. Ainsi, le Tribunal de grande instance de Paris affirme en 1983 que « toute personne qui a été mêlée à des évènements publics peut, le temps passant, revendiquer le droit à l'oubli » et « ce droit à l'oubli qui s'impose à tous, y compris aux journalistes, doit également profiter à tous, y compris aux condamnés qui ont payé leur dette à la société et tentent de se réinsérer »[14]. Dans des termes proches de ce premier jugement, le même tribunal affirme en 1987 que « toute personne qui s'est trouvée associée à un évènement public, même si elle n'en a pas été la protagoniste, est fondée à revendiquer un droit à l'oubli et à s'opposer au rappel d'un épisode de son existence dont la relation peut nuire à sa réinsertion »[15]. En revanche, en 1990, la Cour de cassation met en évidence à l'encontre de la revendication d'un droit à l'oubli, un critère déterminant que constitue la licéité de la première divulgation des faits et qui conduit à débouter les demandeurs. En effet, le caractère public des débats judiciaires leur est opposé pour rejeter leurs prétentions. Dans l'espèce jugée en 1990, la cour précise que ni le droit à la vie privée, ni le droit à l'oubli ne sont invocables : « les faits touchant à la vie privée d'une personne ayant été livrés en leur temps à la connaissance du public par des comptes rendus de débats judiciaires, parus dans la presse locale,

---

12 Ainsi, la Cour d'appel de Versailles précise que, quel que soit le caractère douloureux du rappel d'un passé particulièrement éprouvant pour elle, et « sa revendication légitime d'un droit à l'oubli », Mme F. n'est pas fondée à se prévaloir d'une atteinte portée à sa vie privée par la diffusion du film Fait d'hiver. (Cour d'appel, Versailles, Chambre civile, 26 janvier 2006, n°04/0733). Quant à la Cour d'appel de Montpellier, elle précise en 1997 « si nul droit à l'oubli ne peut être reconnu de manière absolue, il appartient au juge de se prononcer en fonction des circonstances de l'espèce, en tenant compte, certes, du droit pour un journal d'apporter une information libre, complète et objective à son public, mais également de la gravité des faits et du temps écoulé depuis leur commission ainsi que des efforts de réinsertion des personnes anciennement condamnées, dès lors qu'ayant purgé leur peine, elles peuvent légitimement s'opposer au rappel de leurs actes passés, si un tel rappel ne répond à aucune nécessité d'ordre éthique, historique ou scientifique » (Cour d'appel, Montpellier, Chambre 1 section A O, 8 avril 1997, Juris-Data n° 1997-034039).

13 Pour un exposé plus détaillé de la jurisprudence relative aux docu-dictions, voir notamment A. Lucas- Schloetter, Nature du droit d'auteur, Droit d'auteur et droits de la personnalité, JCl. Civil Annexes, Fasc. 1118, n° 24 s. et J.-C. Saint-Pau, Jouissance des droits civils, Droit au respect de la vie privée, Régime, Atteinte à la vie privée, JCl. Civil Code, Fasc. 15, n° 25 s.

14 TGI Paris, 20 avril 1983, JCP 1985, II. 20434, obs. Lindon ; Paris, 24 février 1984, Gaz. Pal., 2. 370.

15 TGI Paris, Chambre 1, 25 mars 1987, Juris-Data n°1987-040634 ; D. 1988, Somm. 198, obs. Amson. Avant ces jugements, un ancien arrêt de la Cour de cassation évoque la nécessité de l'oubli, sans utiliser le terme : « les publications tardives survenant à un moment où elles ont réalisé tout effet utile, ne peuvent plus en produire d'autre que de reprendre incessamment et sans merci, devant l'opinion publique, ceux qui, dans leur propre personne ou dans celle des leurs, ont expié devant la justice ». Cass. Crim. 29 avril 1897, S. 1898, I, 473, note E. Meynial.

ils avaient ainsi été licitement révélés et partant, échappaient à la vie privée ». De plus, « dès lors que les faits touchant à la vie privée d'une personne ayant fait l'objet après la guerre d'un procès pour son attitude pendant l'occupation avaient été licitement révélées à la connaissance du public par les débats judiciaires, la personne qui en est l'objet ne peut se prévaloir d'un droit à l'oubli pour empêcher qu'il en soit de nouveau fait état »[16]. La Cour confirme cette position en 2004 en soulignant dans une autre espèce qu'il est question de « la relation de faits publics déjà divulgués »[17].

7. Ces décisions aboutissent à la solution suivante : l'évocation du passé judiciaire d'une personne n'est pas en elle-même une atteinte à la vie privée en raison de la divulgation licite des faits résultant du débat judiciaire. En revanche, l'œuvre qui dévoilerait davantage d'éléments que ceux déjà révélés peut porter atteinte à ce droit[18]. Sous cette réserve, le droit à la vie privée ne peut donc pas être invoqué par les personnes condamnées contre la nouvelle relation des évènements auxquels elles ont été associées. Face à cette limite du droit à la vie privée, le droit à l'oubli constitue un autre argument contentieux, mais les juridictions considèrent qu'il s'agit d'une cause juridique insuffisante face à la liberté d'expression.

8. De manière plus précise, il faut souligner que le risque judiciaire pour les auteurs souhaitant exploiter un élément du passé judiciaire d'autrui n'est pas réduit à néant. Les juridictions réalisent une balance des intérêts pour chaque espèce. Sont pris en considération : la dimension historique des faits, leur actualité ou leur ancienneté, la nature de l'infraction, l'intérêt légitime du public à être informé, ou le seul objectif d'agrément du public[19]... Les termes du jugement du TGI de Paris du 14 janvier 2013, dans l'affaire des « paras de Francazal », confirment la prise en compte de ces éléments. Rappelant que le droit à la vie privée et le droit à l'information ont la même valeur normative, le tribunal recherche la solution la plus protectrice de l'intérêt le plus légitime. En l'espèce, il souligne que l'émission traite d'un sujet d'intérêt général, « s'agissant de relater une affaire judiciaire ayant à l'époque pris le caractère d'un évènement public, que les images de E. B. ne sont pas attentatoires à sa dignité », que « les faits (...) ont été licitement révélés au public par les comptes rendus des débats judiciaires de sorte qu'une nouvelle relation de ces faits publics déjà divulgués ne peut être considérée comme sans justification légitime, même si elle ne se rattache pas directement à un évènement d'actualité ou aux nécessités de l'information exclusive de toutes préoccupations commerciales ». En outre, le documentaire « ne révèle (...) aucun élément de la vie actuelle de E. B ». Au terme de ce raisonnement, ayant réfuté l'atteinte au droit à l'image et au droit à la vie privée, le TGI de Paris

---

16 Cour de cassation, Civ. 1ère, 20 novembre 1990, n°89-12.580, Bull., JCP 1992. II. 21908, obs. Ravanas : il s'agit en l'espèce du rappel, dans un livre, d'une condamnation pénale. V. aussi TGI Paris, Référé, 27 août 1991, JurisData n°1991-044959.

17 Cour de cassation, Civ. 2e, 3 juin 2004, n°03-11.533, Juris-Data n°2004-023913. Ainsi, il semble que désormais la seule existence d'une divulgation antérieuresuffise, sans exiger son caractère licite.

18 V. par exemple, TGI Nanterre, Chambre 1, 5 octobre 2006, Juris-Data n°2006-322357.

19 V. A. Fourlon, « Toute ressemblance avec des personnages existant ou ayant existé... » est-elle constitutive d'une atteinte aux droits de la personnalité ? Etude de la jurisprudence rendue en matière de fictions du réel, Communication Commerce électronique, mars 2007, étude 5, n°27. Cet auteur évoque précisément le droit à l'oubli comme un « contrepoids de l'épuisement du droit à invoquer le respect de sa vie privée dans l'hypothèse de faits publiquement et licitement relatés » (n°23).

rejette également l'argumentation fondée sur le droit à l'oubli en faisant primer le droit à l'information. Selon cette juridiction, « dès lors que le reportage litigieux révèle à la connaissance du public des faits qui ont donné lieu à un débat judiciaire, puis à une condamnation définitive des protagonistes, dont E. B., que le réalisateur n'a pas manqué à ses devoirs de prudence et d'objectivité dans la relation des faits commis par le demandeur et dans la description qu'il fait de ce dernier, lequel au demeurant ne conteste pas la réalité des informations contenues dans l'émission, le demandeur encore détenu au titre de cette condamnation ne saurait invoquer un droit à l'oubli qui n'est consacré par aucun texte et qui, en l'espèce, ne peut prévaloir sur le droit du public à une information libre, complète et objective sur une affaire pénale ».

9. Ce jugement est représentatif de la tendance récente de la jurisprudence judiciaire à faire pencher la balance du côté de la liberté d'expression, ou plus exactement en faveur du droit à l'information du public. Cette liberté bénéficie également d'une jurisprudence constitutionnelle qui lui est favorable.

II- La confrontation de la liberté d'expression et du droit à l'oubli à la lumière de la jurisprudence constitutionnelle

10. La jurisprudence constitutionnelle sur l'*exceptio veritatis*, c'est-à-dire le procédé permettant à la personne poursuivie pour diffamation de prouver la véracité des faits allégués, est particulièrement éclairante. Saisie d'une question prioritaire de constitutionnalité, le Conseil constitutionnel s'est prononcé sur la conformité à la Constitution de l'article 35 b) de la loi du 2 juillet 1881. Cette disposition prévoit que la vérité des faits diffamatoires ne peut être prouvée « lorsque l'imputation concerne la vie privée de la personne (ou) (...) se réfère à un fait constituant une infraction amnistiée ou prescrite, ou qui a donné lieu à une condamnation effacée par la réhabilitation ou la révision ». Selon la décision du Conseil constitutionnel du 7 juin 2013[20], cette interdiction « vise sans distinction, dès lors qu'ils se réfèrent à un fait constituant une infraction amnistiée ou prescrite, ou qui a donné lieu à une condamnation effacée par la réhabilitation ou la révision, tous les propos ou écrits résultant de travaux historiques ou scientifiques ainsi que les imputations se référant à des événements dont le rappel ou le commentaire s'inscrivent dans un débat public d'intérêt général ; (...) par son caractère général et absolu, cette interdiction porte à la liberté d'expression une atteinte qui n'est pas proportionnée au but poursuivi ; (...) ainsi, elle méconnaît l'article 11 de la Déclaration de 1789 ». Dans cette hypothèse de conflit entre liberté d'expression et droit à l'oubli, sont à l'œuvre non seulement l'écoulement du temps mais également le choix du législateur d'appliquer une mesure d'amnistie ou de prévoir une prescription. Donc il ne s'agit pas tant ici de revendiquer un droit à l'oubli propre aux personnes calomniées que de déterminer la portée et les limites des mécanismes d'oubli que constituent l'amnistie et la prescription.

11. Par ailleurs, le Conseil constitutionnel a eu l'occasion de préciser dans une décision antérieure que l'article 35 c) de la loi du 2 juillet 1881 qui interdit d'apporter la preuve de faits

---

20 Décision n°2013-319 QPC du 7 juin 2013, comm. A. Lepage, Communication Commerce électronique, septembre 2013, comm. 93.

remontant à plus de dix ans, en cas de poursuite pour diffamation, est inconstitutionnel[21]. Cette disposition résulte plus précisément d'une ordonnance de 1944 ayant réformé la loi sur la presse : l'oubli est alors imposé pour répondre à un objectif de paix sociale et l'exceptio veritatis ne peut jouer. L'objectif de cette disposition est en effet, selon le Conseil constitutionnel, « d'éviter que la liberté d'expression ne conduise à rappeler des faits anciens portant atteinte à l'honneur et à la considération des personnes qu'elles visent ; (...) la restriction à la liberté d'expression qui en résulte poursuit un objectif d'intérêt général de recherche de la paix sociale ». Toutefois, ce régime est contestable notamment parce qu'il peut gêner la poursuite de travaux historiques, il est censuré par le Conseil constitutionnel en ce qu'il aboutit à « une conciliation qui n'est pas équilibrée entre la liberté d'expression et la recherche d'un droit à l'oubli »[22].

12. La jurisprudence constitutionnelle est ainsi particulièrement protectrice de la liberté d'expression. Il convient de souligner que dans ses décisions, le Conseil constitutionnel n'utilise pas explicitement la formule « droit à l'oubli ». En outre, dans certaines des hypothèses visées par la loi de 1881, le débat sur l'existence d'un droit à l'oubli (de la personne calomniée) se double nous semble-t-il d'une dimension de « droit de l'oubli » lorsqu'il est question de faits prescrits ou amnistiés : la solution n'est pas alors véritablement comparable au sujet qui nous intéresse. Seule la disposition relative à l'écoulement d'un délai de dix ans relevait à notre sens d'un véritable droit à l'oubli dans la mesure où elle s'appliquait à des faits non soumis à une mesure d'effacement telle que l'amnistie. La décision du 20 mai 2011 est donc particulièrement éclairante car elle porte à proprement parler sur les effets de l'écoulement du temps. Elle démontre que le juge constitutionnel refuse d'admettre une restriction de la liberté d'expression formulée de manière trop large et justifiée par le seul passage du temps. En protégeant ainsi la liberté d'expression, le Conseil constitutionnel ne ferme-t-il pas la porte à un éventuel droit à l'oubli pour les personnes condamnées ? Il faudrait pour formaliser un tel droit que son invocation soit strictement encadrée pour ne pas encourir de censure du Conseil constitutionnel notamment[23]. Ce droit apparaît du moins pour l'heure doublement fragilisé par la primauté accordée par le juge judiciaire comme par le juge constitutionnel à la liberté d'expression.

13. Au-delà des termes généraux de la confrontation du droit à l'oubli et de la liberté d'expression, une interrogation plus précise doit également être formulée sur le sujet qui nous intéresse : les dispositions législatives propres aux détenus peuvent-elle fonder un droit à l'oubli spécifique ?

---

21 Décision n° 2011-131 QPC du 20 mai 2011, comm. A. Lepage, Communication Commerce électronique, juillet 2011, comm. 68.

22 Commentaire de la décision n°2013-319 QPC du 7 juin 2013, disponible sur le site du Conseil constitutionnel, p. 18. Ce commentaire vise également la décision n° 88-244 DC du 20 juillet 1988 qui évoque si ce n'est un droit à l'oubli du moins l'oubli lui-même. Cette dernière, relative à une loi d'amnistie, précise que le législateur peut rechercher, « par l'exercice de la compétence que la Constitution lui reconnaît en matière d'amnistie », « l'oubli de certains faits et l'effacement de leur caractère répréhensible », « dans un souci d'apaisement politique ou social ».

23 La Cour européenne des droits de l'homme n'admettrait pas non plus une restriction excessive de la liberté d'expression au nom du droit à l'oubli. Voir ses critiques sur l'exceptio veritatis et l'écoulement du temps, CEDH, 7 nov. 2006, n° 12697/03, Mamère c/ France, D. 2007, jurispr. p. 1704, note J.-P. Marguénaud.

Section 2- Un droit à l'oubli spécifique pour les détenus ?

14. La loi pénitentiaire du 24 novembre 2009[24] contient une disposition spécifique au droit à l'image des détenus. L'article 41 de ce texte affirme en effet que :

15. « Les personnes détenues doivent consentir par écrit à la diffusion ou à l'utilisation de leur image ou de leur voix lorsque cette diffusion ou cette utilisation est de nature à permettre leur identification.

16. L'administration pénitentiaire peut s'opposer à la diffusion ou à l'utilisation de l'image ou de la voix d'une personne condamnée, dès lors que cette diffusion ou cette utilisation est de nature à permettre son identification et que cette restriction s'avère nécessaire à la sauvegarde de l'ordre public, à la prévention des infractions, à la protection des droits des victimes ou de ceux des tiers ainsi qu'à la réinsertion de la personne concernée. Pour les prévenus, la diffusion et l'utilisation de leur image ou de leur voix sont autorisées par l'autorité judiciaire ».

17. Si le premier alinéa de cette disposition ne fait que réaffirmer le droit à l'image dont les détenus disposent comme les autres individus, le second alinéa attribue à l'administration pénitentiaire la mission particulière de s'opposer à l'utilisation de l'image d'un détenu, notamment lorsque la réinsertion de celui-ci est en cause, et malgré son consentement. Par là-même, le texte envisage les effets à venir de cette utilisation et donc anticipe en quelque sorte sur la nécessité de préserver en amont le droit à l'oubli. Il crée une forme de « protection administrative »[25] du droit à l'image, à côté des protections civile et pénale résultant l'une de l'article 9 du code civil, l'autre de l'article 226-1 du code pénal.

18. Cette disposition originale a donné lieu à un développement contentieux devant le Tribunal administratif de Paris. En l'espèce, un documentaire tourné dans des établissements pénitentiaires avec l'accord de l'administration pénitentiaire a fait l'objet d'une autorisation de diffusion de la part du ministre de la justice sous réserve, pour les diffusions télévisuelles, que l'anonymat physique et patronymique des personnes détenues apparaissant dans le film soit préservé. Cette restriction est contestée par la société productrice et la réalisatrice devant la juridiction administrative. Or le motif de cette décision n'est nullement précisé, la motivation de la décision n'étant faite que par référence aux termes généraux de la loi, c'est-à-dire en mentionnant des considérations « liées à la sauvegarde de l'ordre public, à la prévention des infractions, à la protection des droits des victimes ou de ceux des tiers ainsi qu'à la réinsertion de la personne concernée ». Le Tribunal administratif considère qu'« il ne ressort (...) nullement du contenu de ce documentaire que celui-ci serait de nature à faire obstacle à la réinsertion des personnes concernées ; qu'en effet, le film n'aborde à aucun moment les faits pour lesquels les personnes détenues qui témoignent ont été condamnées, ne décrivant que leurs conditions de détention, en particulier les changements intervenus dans leur quotidien du fait de leur transfert de l'ancienne maison d'arrêt de Rennes vers le nouveau centre pénitentiaire de Rennes-Vezin ; que, par ailleurs, il ne comporte aucune image dégradante pour les intéressés dont l'anonymat

---

24 Loi n°2009-1436, JORF du 25 novembre 2009, p. 20192.

25 V. P. Poncela, Les liaisons dangereuses du droit à l'image et du droit à l'information du public, Chronique de l'exécution des peines, RSC juillet/septembre 2012, p. 651.

patronymique est au demeurant préservé »[26]. Dès lors, l'administration pénitentiaire ne peut restreindre par principe la diffusion d'images de détenus filmés à visage découvert et y ayant consenti. La décision du ministre de la justice est annulée alors même que son raisonnement était sous-tendu par le droit à l'oubli des personnes détenues. Ce droit ne peut être invoqué par l'administration pénitentiaire à l'encontre du droit des détenus sur leur propre image[27].

19. L'article 41 de la loi pénitentiaire a été invoqué également dans le contentieux qui nous intéresse ici, celui des documentaires-fictions, en soulevant un intéressant problème d'interprétation et de délimitation de son champ d'application. M. E. B. fait ainsi valoir devant le TGI de Paris, dans l'affaire jugée le 14 janvier 2013, que cet article pourrait fonder un droit à l'image propre aux personnes condamnées, et que cette disposition ne vise pas exclusivement les images filmées en détention. Ce droit à l'image spécifique pourrait au demeurant être l'instrument d'un droit à l'oubli propre aux personnes condamnées : celles-ci pourraient pour exercer ce droit s'opposer à la diffusion de leur image. Cette interprétation extensive de l'article 41 semble néanmoins incohérente à plusieurs titres : tout d'abord parce que le texte même qui contient la disposition discutée est bien une loi pénitentiaire, ensuite parce que l'autorité compétente pour s'opposer à la diffusion et l'utilisation de l'image relève de l'administration pénitentiaire, enfin, parce que si l'alinéa 2 de cet article envisage les personnes condamnées ce n'est que par opposition aux prévenus envisagés in fine par cette disposition. Il nous semble donc que, même si le texte ne le mentionne pas expressément, ce sont précisément les images captées dans les lieux de détention qui sont concernées et non toute image d'une personne condamnée. Le tribunal se prononce en ce sens en affirmant que l'article 41 ne s'applique « qu'aux images qui représentent des personnes, prévenues ou condamnées, en situation de détention et n'ont pas vocation à créer au profit de celles-ci, s'agissant de leur image captée en dehors de tout contexte pénitentiaire, une protection supérieure à celle qui est accordée à toute personne au moyen de l'article 9 du code civil ». Une autre interprétation nécessiterait de prévoir une modalité de contrôle préalable par l'administration pénitentiaire de toute œuvre incluant les images de personnes condamnées et détenues. Si l'on souhaite mener une interprétation aussi constructive de l'article 41 de la loi pénitentiaire et garantir plus fermement ainsi le droit à l'oubli des personnes détenues, encore faut-il mettre en place une procédure en ce sens[28].

20. Malgré ces interprétations audacieuses, le droit à l'oubli n'est pas accueilli favorablement par les juridictions. En revanche, ce droit est examiné avec intérêt à l'heure actuelle par des institutions qui plaident pour sa reconnaissance ou au moins pour une meilleure prise en compte des droits des personnes condamnées.

---

26 TA Paris, n°1201622/7-1, Société Candala Productions et Mme R., AJDA 2012, p. 1436 ; S. Slama, Contrariété à la loi pénitentiaire d'une autorisation de diffusion télévisuelle d'un documentaire conditionnée à l'anonymat physique et patronymique des détenus in Lettre « Actualités Droits-Libertés » du CREDOF, 14 août 2012

27 V. Question écrite n° 960 de Mme Maryvonne Blondin, JO Sénat 23 février 2012, p. 477.

28 V. P. Poncela, Les liaisons dangereuses du droit à l'image et du droit à l'information du public, Chronique de l'exécution des peines, RSC juillet/septembre 2012, p. 658. L'association Ban public défend cette interprétation extensive de l'article 41 de la loi pénitentiaire.

Section 3 - Un droit condamné à la *soft law* ?

21. Adoptée le 10 juillet 2003, la recommandation REC(2003)13 du Comité des ministres du Conseil de l'Europe est relative à la diffusion d'informations par les médias en relation avec les procédures pénales. Elle énonce divers principes dont l'un est relatif aux reportages réalisés à la suite de l'exécution des peines. Il précise : « Afin de ne pas porter préjudice à la réintégration dans la société des personnes qui ont purgé une condamnation, le droit à la protection de la vie privée en application de l'article 8 de la Convention devrait inclure le droit à protéger l'identité de ces personnes en liaison avec le délit qu'elles ont antérieurement commis une fois qu'elles ont purgé leur condamnation, sauf si ces personnes ont consenti explicitement à la divulgation de leur identité ou si ces personnes et le délit qu'elles ont antérieurement commis sont un sujet d'intérêt public ou sont redevenus un sujet d'intérêt public » (Principe 18). Ce principe reflète les préoccupations relatives à l'oubli du passé judiciaire vis-à-vis des médias.

22. Au niveau national, les autorités administratives indépendantes saisies par les personnes condamnées ou les associations expriment la nécessité de préserver, au-delà des textes, les droits de ces personnes en particulier lorsqu'elles sont encore en détention. Ainsi, le Conseil supérieur de l'audiovisuel a adopté plusieurs décisions à ce sujet et collabore aujourd'hui avec le Contrôleur général des lieux de privation de liberté pour faire progresser les droits des personnes condamnées.

23. Le Conseil supérieur de l'audiovisuel est intervenu à plusieurs reprises pour inciter les chaînes de télévision à prendre en compte les conséquences de la diffusion de leurs programmes sur les personnes concernées. Il a par exemple adopté une décision en Assemblée plénière le 7 janvier 2010 au sujet de l'émission *Faites entrer l'accusé*. Il considère que « les médias ont une grande latitude pour relater les faits tirés d'affaires judiciaires jugées, sous réserve notamment du respect des droits des victimes consacré par la loi du 29 juillet 1881 sur la liberté de la presse ». Mais il invite les chaînes à prendre des précautions supplémentaires afin que la vie privée présente des personnes condamnées soit respectée[29]. En outre, cette décision évoque in fine et implicitement le droit à l'oubli : « Le Conseil souhaite également que d'autres précautions soient prises par les éditeurs et producteurs de l'émission, afin de préserver les possibilités de réinsertion des personnes condamnées et améliorer leur sécurité ainsi que celle de leur famille ». A propos de la même émission, l'Assemblée plénière du Conseil supérieur de l'audiovisuel s'est prononcée à nouveau le 9 octobre 2012[30]. Elle rappelle les exigences générales résultant de la loi et de la

---

29 « Afin de garantir le droit à la vie privée, le Conseil considère qu'aucun élément relatif à la vie présente de la personne condamnée ne doit être diffusé ou révélé à l'antenne à cette occasion. Lorsque cette personne s'exprime dans l'émission mais demande la protection de son image et ne souhaite pas pouvoir ensuite être reconnue, cette protection doit être pleinement garantie par tout moyen adapté, y compris si nécessaire par la transformation de la voix de l'intéressé ».

30 Le Conseil est intervenu auprès de France Télévisions à la suite de la diffusion, le 13 mai 2012 sur France 2, de l'émission Faites entrer l'accusé consacrée à l'assassinat de Joël Deprez. Il considère que la liberté de communication et d'information du public n'exonère pas les éditeurs de respecter les droits des personnes évoquées à l'antenne, en veillant à ne pas porter atteinte à leur vie privée ni à leur droit à l'image tel qu'il est défini par l'article 9 du Code civil et par la jurisprudence, et pour les personnes incarcérées, encadré par l'article 41 de la loi du 24 novembre 2009, aux termes duquel celles-ci « doivent consentir par écrit à la diffusion ou à l'utilisation de leur image ou de leur voix

jurisprudence quant au respect de la vie privée et précise que l'article 41 de la loi pénitentiaire contient des termes spécifiques aux détenus.

24. Une critique doctrinale consiste à s'interroger sur la compétence – et la légitimité – du CSA à agir auprès des chaînes de télévision pour les inciter à davantage prendre en compte les droits des personnes condamnées. C'est minorer là à la fois la mission d'une autorité de régulation et l'intérêt de l'existence même des autorités indépendantes pour relayer des demandes sociales face aux intérêts économiques. Rappelons en outre que la loi de 1986 donne au CSA un pouvoir de recommandation pour la mise en œuvre des principes qu'elle énonce[31] et que son action en la matière relève aussi du registre de la déontologie.

25. Dans son rapport 2010, le CSA mentionne précisément la demande sociale qui l'a conduit à développer cette action. Il a en effet reçu plusieurs plaintes au sujet d'émissions relatant des affaires judiciaires passées qui mettraient à mal les possibilités de reconstruction et de réinsertion des personnes condamnées et de leurs proches, ainsi que le travail de deuil des familles de victimes[32]. Ces plaintes émanaient du Contrôleur général des lieux de privation de liberté, d'associations (l'Aumônerie catholique des prisons, la section de Toulouse de la Ligue des droits de l'homme, l'association Ban public), ainsi que de personnes condamnées ou de victimes et de leurs proches. Plusieurs de ces plaintes concernaient France 2. Après ces saisines, le groupe de travail « Déontologie des contenus audiovisuels », au sein du CSA, a engagé une réflexion sur le droit à l'oubli. Par ailleurs, le CSA a auditionné le CGLP et l'association Ban public en 2011.

26. La signature le 2 août 2011 d'une convention entre le CSA et le Contrôleur général des lieux de privation de liberté[33] témoigne de cette attention particulière portée au droit à l'oubli des personnes condamnées, sachant qu'en détention, elles peuvent subir des brimades de la part de co-détenus lors des diffusions de ces émissions, et qu'une fois libérées, leurs difficultés de réinsertion sont accrues.

27. Ainsi, s'il n'est consacré ni par les textes ni par la jurisprudence, le droit à l'oubli du passé judiciaire des personnes condamnées suscite un intérêt tout particulier des autorités indépendantes compétentes. La demande sociale de reconnaissance d'un droit à l'oubli du passé

---

lorsque cette diffusion ou cette utilisation est de nature à permettre leur identification » (Assemblée plénière, décision du 9 octobre 2012).

31 Ainsi B. Montels s'interroge sur « les fondements juridiques qui habilitent le CSA à intervenir auprès des chaînes de télévision lorsqu'il estime qu'un programme porte atteinte à la vie privée ou au droit à l'image d'une personne (...) Certes, dans la loi de 1986, dite sur la « liberté de communication », il dispose de certains pouvoirs pour contrôler la déontologie des programmes (...), mais ceux-ci ont des objectifs d'intérêt général (respect de la dignité humaine, protection de l'enfance et de l'adolescence, sauvegarde de l'ordre public, lutte contre les discriminations, interdiction de l'incitation à la haine ou à la violence). Aussi, en quoi une autorité administrative indépendante est-elle encore légitime pour défendre des droits aussi attachés à la personne que la vie privée et le droit à l'image protégés par l'article 9 du Code civil ? Seul le titulaire de ces droits de la personnalité doit pouvoir agir devant des tribunaux qui seront les mieux à même d'appliquer une jurisprudence qui aujourd'hui a institué plusieurs critères – en particulier ceux des « faits publics » et de « l'événement d'actualité » – permettant une véritable mise en balance des intérêts en présence. B. Montels, Un an de droit de l'audiovisuel, Communication Commerce électronique, n°6, 2013, chron. 6, n°15.

32 Rapport du Conseil supérieur de l'audiovisuel, 2010, p. 111.

33 http://www.cglpl.fr/wp-content/uploads/2009/03/Convention-CSA1.pdf

judiciaire n'est donc que très partiellement satisfaite : sa prise en compte par des autorités indépendantes n'aboutit pas à une formalisation qui seule donnerait à ce droit un fondement textuel et jurisprudentiel solide.

Conclusion

28. Le cas particulier des personnes condamnées permet de formuler les remarques conclusives et propositions suivantes dans une double démarche, d'analyse du droit positif et de droit prospectif.

De lege lata. Du « droit à l'oubli » en général et du « droit à l'oubli du passé judiciaire » en particulier.

29. La problématique soulevée par le passé judiciaire des personnes condamnées reflète les questions qui traversent la recherche sur le droit à l'oubli dans son ensemble : le droit à l'oubli doit-il être reconnu comme un corollaire du droit à la vie privée ou comme un droit autonome ? Le cas analysé fait nettement apparaître les limites du droit à la vie privée, l'exploitation du passé judiciaire n'étant pas considérée en tant que telle comme une atteinte à ce droit ; toutefois, l'opposition à la diffusion de l'image de la personne constitue l'instrument de mise en œuvre de ce droit à l'oubli. Cette hypothèse révèle aussi une demande sociale pour tirer des effets de l'écoulement du temps, effets qui consisteraient à obtenir si ce n'est le silence, du moins l'anonymisation des évènements relatés afin de ne pas exploiter le passé sans cesse et sans égard pour le devenir des personnes associées à ces faits. Ce sujet permet aussi de s'interroger sur le rôle des autorités publiques : le droit à l'oubli doit-il être considéré comme un droit de la personnalité invocable par la seule personne intéressée ? Faut-il consacrer la puissance publique comme garante de ce droit ? Dans l'hypothèse des personnes condamnées, a été évoqué le rôle particulier de l'administration pénitentiaire et celui des autorités indépendantes que sont le CSA et le CGLPL.

De lege feranda. Quel peut être l'avenir du droit à l'oubli pour les personnes condamnées ?

30. Tout d'abord, il est possible d'envisager un statu quo, solution la plus probable à notre sens. Au mieux dans ce cas, le droit à l'oubli gagnerait du terrain en soft law en faisant l'objet de multiples recommandations et avis d'instances non juridictionnelles. Dans ce cas, la prise en compte du droit à l'oubli des personnes condamnées pourra progresser par le développement de bonnes pratiques ou de principes déontologiques. La suggestion consiste ici non pas à formuler une interdiction de ce type d'émissions mais à envisager une charte du droit à l'oubli dans le secteur audiovisuel et pour la presse écrite, sur le modèle de la charte de la diversité dans ce secteur, ou de la charte du droit à l'oubli numérique. Pourrait-on de surcroît envisager en particulier de soumettre les chaînes de télévision du service public à des engagements permettant une meilleure prise en compte du droit à l'oubli ? Le service public formulerait ainsi des principes plus exigeants, des précautions supplémentaires telles que les envisagent le CSA. Certes une telle différence de traitement entre les chaînes publiques et privées pourrait constituer une rupture d'égalité mais il s'agirait d'une démarche volontaire afin de renforcer l'identité du service public audiovisuel et ses principes déontologiques. La proposition peut sembler bien ambitieuse si l'on rappelle que c'est précisément une chaîne du service public, France 2, qui est à l'origine de plusieurs décisions du CSA.

31. Ensuite, imaginons que cette prolifération en soft law constitue seulement la première étape d'un processus de formalisation. Si le droit à l'oubli des personnes condamnées était consacré, deux voies seraient envisageables.

32. La première consisterait à ne consacrer qu'un droit à l'oubli réservé aux personnes condamnées, dès lors, il faudrait imaginer une disposition législative qui imposerait de ne pas faire mention de faits relevant du passé judiciaire d'un individu. Toutefois, il serait nécessaire de délimiter préciser le champ de cette disposition, en indiquant par exemple que la prohibition ne concernerait que les reprises d'informations qui seraient réalisées sans le consentement de la personne autorisée, sans lien avec l'actualité, ni avec une démarche historique ou scientifique. Comme nous l'avons vu, les restrictions à la liberté d'expression peuvent être censurées dans le cadre du contrôle de constitutionnalité - sauf à envisager l'inscription d'un droit à l'oubli dans la Constitution - ou de conventionnalité. L'écriture d'une telle disposition sera donc particulièrement délicate ; d'autant qu'il faudra envisager le délai permettant d'invoquer le droit à l'oubli et de considérer qu'un fait n'est plus d'actualité[34]. Sans doute, peut-on envisager de réformer la loi pénitentiaire, comme le propose P. Poncela, mais dans ce cas, s'agira-t-il de faire bénéficier de cette disposition toutes les personnes condamnées ou seulement celles qui sont détenues ? En outre, la proposition d'une information préalable et d'un droit d'opposition de l'administration pénitentiaire nous semble peu réaliste car difficile à mettre en œuvre en pratique pour cette administration déjà sous tension. Comment consacrer concrètement le droit à l'oubli des personnes condamnées autrement que par l'interdiction de diffuser des images issues de leur passé judiciaire sans leur autorisation ? L'anonymat et le pseudonymat[35] peuvent être envisagés comme des solutions intermédiaires qui tempèreraient en outre la dramatisation des émissions visées[36].

33. La seconde solution consisterait à envisager le droit à l'oubli de manière plus large en considérant que la consécration d'un tel droit pour les seules personnes condamnées n'est pas pertinente. Si leur situation a été ici isolée, elle mérite d'être replacée à présent dans le cadre d'ensemble de ce rapport. Peut-on envisager une reconnaissance sectorielle ou catégorielle du droit à l'oubli ? Techniquement, l'idée est séduisante car il est sans doute plus aisé d'entamer une démarche propre aux personnes condamnées et de modifier la loi de 1881 sur la liberté de la

---

34 Ainsi la Cour d'appel de Douai a eu l'occasion de préciser que le droit à l'oubli ne peut être invoqué que pour la relation de faits lointains et anciens, ce qui n'est pas le cas pour un meurtre commis en 2002 et jugé en 2005. V. CA Douai, Chambre 3, 13 octobre 2007, n° 07/02141, Dalloz Jurisprudence. V. aussi TGI Paris, Chambre 17, 0 décembre 2002, JurisData n°2002-216393 (pour un procès ayant eu lieu seulement trois ans avant la publication du document litigieux).

35 V. F. Girard, Sens et possibilités d'un « droit à l'oubli » aux Etats-Unis, Chapitre 2/ Troisième partie

36 L'association Ban public formule plusieurs propositions à propos du droit à l'oubli. Elle préconise que la personne détenue ou ex-détenue, au nom du droit à l'image, de sa vie privée et du droit à l'anonymat, puisse s'opposer à la diffusion des films, émissions, documentaires et autres moyens de diffusion de son image, de sa voix et de son histoire. La personne concernée doit donc être informée du projet d'une telle diffusion. L'association considère qu'« en tout état de cause, des moyens d'anonymisation doivent être utilisés : floutage des visages, transformation des voix, changements des noms et des lieux etc. ». Enfin, elle suggère que soit développée une réflexion déontologique entre les professionnels de la presse et des associations de défense des personnes détenues et ex-détenues pour déterminer les règles d'équilibre à respecter entre ses éventuels intérêts antagonistes. Document disponible sur http://prison.eu.org/IMG/pdf/droit_a_l_oubli.pdf

presse en ce sens. Il existe néanmoins des interactions entre les hypothèses évoquées : par exemple, des individus ayant fait l'objet de poursuite pénale sans être condamnés pourraient-ils se prévaloir du mécanisme ? Est-il pertinent de réserver un traitement particulier aux personnes condamnées (au regard de leur vulnérabilité en détention et de leur difficile réinsertion après leur libération) alors que d'autres citoyens ne peuvent faire valoir leur droit à l'oubli face à un passé qui, sans être pénalement répréhensible ou réprimé, resurgit par exemple sur internet ? Le risque à l'heure actuelle est moins de voir consacré le droit à l'oubli des personnes condamnées qu'à l'inverse de voir le droit à l'oubli numérique progresser sans entraîner avec lui la consécration du même droit dans d'autres situations n'intéressant pas internet. Or, il faut enfin insister sur la nécessité de s'intéresser aux retombées d'une reconnaissance sectorielle du droit à l'oubli telle qu'elle est envisagée actuellement : les réflexions en cours, au sujet du projet de règlement européen, notamment au sein de la CNIL, envisagent essentiellement, si ce n'est exclusivement, le droit à l'oubli dans sa facette numérique. Pourtant ce droit révèle des interrogations qui dépassent ce seul champ et, en toute hypothèse, intéresse la résurgence du passé. Il conviendrait de ne négliger ni les autres supports de la liberté d'expression qui, quoique complétés et concurrencés par internet, n'en demeurent pas moins des vecteurs importants de communication (presse écrite, télévision...), ni certaines catégories de citoyens pour lesquels l'oubli est une condition de réinsertion.

CHAPITRE 4

« Définir et revendiquer l'oubli : une perspective philosophique »[1]

Introduction

L'expression de « droit à l'oubli » ne peut que surprendre alors que les sociétés humaines sont articulées autour de la préservation du souvenir et de la mémoire. L'essor des outils numériques et les possibilités accrues de stockage, de traitement et de diffusion des traces qui en découlent participent de cette entreprise. Il semble qu'aujourd'hui rien ne peut plus être oublié. Comment dès lors agir ou s'offrir une seconde chance dans un monde où tout est enregistré, sauvegardé et finalement visible et accessible ?

Revendiquer l'oubli serait un moyen de préserver de telles possibilités. Néanmoins, l'expression de « droit à l'oubli » nécessite d'être définie. Un tel droit n'existe pas, à proprement parler, dans le droit positif[2]. De plus, si l'oubli est envisagé comme un mécanisme qui vise la préservation des capacités d'actions individuelles, comment l'articuler aux impératifs de la vie sociale dans le cadre de laquelle les traces peuvent constituer un bien commun ? Il s'agit dès lors de se demander dans quelle mesure les traces participent à des rapports de forces et à des stratégies qui traversent le corps social et comment l'oubli influence ces rapports de force et, dans certains cas, se révèle nécessaire.

Dans le cadre de cette contribution nous poserons cette question dans le cadre de l'essor de la « condition numérique » entendue comme la vie humaine dans son rapport aux outils numériques[3]. Il s'agira, en répondant à cette question, de définir l'oubli comme un droit tout en interrogeant les difficultés de sa mise en pratique. Avant de parvenir à ce point, il est nécessaire de définir l'oubli. Cette première étape permettra de distinguer le souvenir individuel, et la mémoire personnelle, d'une mémoire construite socialement, comme l'histoire, qui implique une sélection. Ce détour par l'histoire et le devoir de mémoire notamment permettront de mettre en lumière le rôle de la mémoire dans les rapports de pouvoir. Nous interrogerons ensuite la place de la mémoire dans les rapports de pouvoir spécifique à la condition numérique et montrerons, dans cette perspective la nécessité de l'oubli afin de préserver les capacités d'action individuelles. Enfin, nous mettrons en abîme cette nécessité avec la pratique de stockage et de traitement des données et en montrerons les difficultés.

---

1 Par Aurélien Faravelon, Attaché temporaire d'enseignement et de recherche, Université Grenoble Alpes, Centre de recherches Philosophie, langage et cognition et laboratoire informatique de Grenoble.

2 Le « droit à l'oubli » fait ainsi l'objet d'un projet de directive européenne.

3 L'expression de « condition numérique » est aujourd'hui fréquemment employée dans la réflexion sur les outils numériques. Jean-François Fogel et Bruno Patino, par exemple, lui consacrent un ouvrage. Voir Fogel, J. F. & Patino, B. La condition numérique Grasset, 2013.

Section 1- La revendication de l'oubli, une revendication surprenant

Ce premier niveau d'analyse entend situer l'oubli par rapport à la mémoire. Il s'agit ici d'établir la mémoire comme un élément nécessaire à l'action du point de vue individuel comme du point de vue politique. Il s'agit aussi d'établir la mémoire comme un phénomène socialement construit et comme un impératif moral au travers de l'exemple du « devoir de mémoire ». Dans cette perspective, l'oubli est le résultat d'un procédé de sélection des éléments que l'on doit conserver.

I- L'oubli, un donné du point de vue subjectif

Dans l'oubli, on tombe. Momentané – comme une « perte de mémoire » - ou permanent, l'oubli constitue une déficience, par opposition à la « mémoire » qui désigne la faculté de ramener un souvenir. Qu'il passe ou qu'il dure, l'oubli gène le discours ou l'action. La mémoire, constituée par l'acquisition de souvenirs et d'habitudes, joue un rôle primordial dans l'apprentissage – qui repose sur la répétition et la mémorisation. Du point de vue biographique, la somme des souvenirs est nécessaire à la définition de l'identité personnelle. Elle permet en effet de rendre compte de ses actes afin de permettre à nos interlocuteurs de nous reconnaître et, au besoin, de nous juger[4]. Dès, lors la mémoire permet d'élaborer une réponse à la question « Qui es tu ? »[5]. Cette question appelle une réponse narrative, qui repose non seulement sur l'articulation du souvenir mais aussi des conditions sociales de l'existence.

Dans le cadre de l'histoire personnelle, l'oubli joue notamment deux rôles. Tout d'abord, la biographie repose sur l'oubli, qu'il prenne la forme de la sélection ou du résultat de la perte de la force des souvenirs avec le temps qui passe. Dans cette perspective, l'oubli peut prendre la forme du refoulement au sens de la psychanalyse freudienne[6]. Il constitue dès lors un mécanisme de protection de l'individu contre ses pulsions. L'oubli est aussi un phénomène proche de la « cicatrisation » : les éléments de la mémoire perdent petit à petit de leur force et tombent dans l'oubli.

Ensuite, l'oubli est potentiellement délétère. Si l'oubli peut être un mécanisme de protection, il peut aussi avoir une origine pathologique, comme les maladies neurodégénératives. Il porte alors atteinte aux capacités et à l'identité d'une personne. Il constitue dès lors une limitation cognitive.

---

4 Nous reprenons ici la définition classique de l'identité personnelle et de son rapport à la mémoire que l'on trouve, notamment, chez John Locke. Voir Locke J., Essai sur l'entendement humain, Paris, Vrin, 2001, II, XXVII, pp. 505-542. Dans ce chapitre, l'auteur définit l'identité personnelle comme la persistance de la mémoire et de la conscience de cette dernière.

5 Dans Les sources du moi, Charles Taylor fait de l'identité une narration produite en à une interpellation adressée à un individu ou que ce dernier peut s'adresser à lui-même. Cette réponse s'appuie non seulement sur les souvenirs d'un individu mais aussi sur le positionnement de ces derniers par rapport aux biens qui motivent l'action. Voir Taylor, C. Les sources du moi : la formation de l'identité moderne Seuil, 1998, p. 46.

6 La définition freudienne du refoulement comme un procédé de protection de l'individu face aux pulsions fait notamment l'objet de la Métapsychologie. Voir Freud, S. Métapsychologie. Folio, 1986.

Dans la perspective du rapport de soi à soi, l'oubli est un fait que nous subissons contre lequel nous luttons dans une certaine mesure. Il n'y a ainsi pas, dans le rapport de l'individu à lui-même, un « droit à l'oubli ». Comme le montre la portée narrative de l'identité personnelle et le procédé de sélection qu'elle implique, il faut dès lors situer un « droit à l'oubli » au niveau des relations interpersonnelles.

II- La mémoire comme nécessité pratique et politique

Si la mémoire constitue, du point de vue individuel, un élément nécessaire à l'action, il est en de même du point de vue social. Ici, « mémoire » doit s'entendre comme l'ensemble des traces qui concernent un groupe d'individus. Ces traces peuvent être constituées des souvenirs des individus ou encore des enregistrements réalisés au moyen de machines et plus généralement de l'ensemble des traces que produisent les activités humaines. Dans cette perspective, l'identité personnelle est une identité socialisée[7].

Le terme de « personne » doit en effet être compris dans son sens juridique de porteur de droits et d'entité pouvant être jugée[8]. Dès lors, l'oubli, compris comme l'effacement ou la perte des traces s'oppose à la possibilité de connaître et de qualifier des actes. Il s'oppose ainsi à la possibilité de rendre la justice entendue comme la possibilité de distribuer les peines et les récompenses et les biens. Dans le cadre d'une procédure judiciaire, par exemple, l'oubli peut prendre le sens de dissimulation auquel s'opposent les mécanismes de l'enquête, du recueil de preuves et de témoignages. Dans le cas de la volonté d'être oublié, la nécessité de la justice limite notre propension à dissimuler au mieux les informations qui donnent une image défavorable de nous-mêmes, au pire, les faits délictueux que nous avons commis.

Les traces, même les plus personnelles en apparence, peuvent dès lors constituer un « bien public ». Cette position devient particulièrement importante avec l'essor de l'économie libérale au XIXe siècle, qui est contemporain de celui de la statistique[9]. Étymologiquement, cette dernière désigne, l'énumération et l'étude des « choses de l'État ». Elle désigne ainsi à la fois la collecte des traces mais aussi, d'un point de vue mathématique, l'analyse de la structure d'un ensemble de données et de l'évolution de cette structure dans un but prédictif. Le perfectionnement des outils mathématiques et des machines de calcul ainsi que l'accroissement du volume de données disponibles font de cette nouvelle discipline un élément nécessaire du maintien de la santé de l'État. La connaissance de l'État devient un élément primordial dans la définition des orientations économiques et politiques notamment. Dès lors, les traces sont des « bien public » puisqu'elles permettent de maintenir les conditions pratiques de l'essor d'une vie publique. Dans la mesure où les liens établis par la statistique peuvent porter sur toutes les choses

---

7 Plutôt qu'une nouvelle définition de l'identité personnelle, nous adoptons ici un nouvel angle de vue. L'identité personnelle au sens de biographie comme l'entend Ch. Taylor, par exemple, est déjà une identité socialisée puisqu'elle repose sur l'énumération d'un ensemble de biens sociaux vers lesquels on souhaite tendre.

8 L'identité est ainsi une identité « d'état civil » qui fait de la personne l'objet d'un jugement. Voir « Qu'est-ce qu'un auteur ? » in Foucault, M. Dits et Ecrits, tome 2 : 1976 - 1988 Gallimard, 2001, texte n°258.

9 Nous reprenons brièvement ici l'analyse que livre Michel Foucault de l'essor du libéralisme économique et des statistiques. Voir Foucault, M. Sécurité, territoire, population : Cours au Collège de France (1977-1978) Seuil, 2004, p. 23 et sq.

et toutes les activités, les limites de ce bien public ne sont pas évidentes. Le « droit à l'oubli », entendue comme la sélection des traces que l'on souhaite voir disparaître contrevient à l'obtention de ce bien public et, potentiellement, à la réalisation des missions de l'État.

Ce qui vaut pour les États vaut aujourd'hui pour les sociétés privées. Les traces qu'elles possèdent sur leurs clients, leur personnel et plus généralement leurs activités, constituent des actifs qu'elles peuvent valoriser soit en les vendant, soit en les utilisant dans le cadre d'opérations publicitaires, soit en les traitant. Le droit à l'oubli s'oppose ainsi à leur stratégie commerciale. Par conséquent, tout comme l'oubli gêne l'action individuelle, il faut identifier un impératif pratique à constituer une mémoire vue comme un bien social.

III- Le devoir de mémoire et l'oubli

La nécessité économique ou juridique des traces ne peut, seule, plaider pour leur conservation dans la mesure où la conservation. Le traitement et la diffusion de certaines traces porte de manière évidente préjudice aux individus qu'elles concernent. Néanmoins, le droit à l'oubli s'oppose à un dernier impératif, moral lui, le « devoir de mémoire ». À la nécessité de se souvenir, ou de combler la déficience que constitue l'oubli, il faut ici substituer « l'injonction à se souvenir »[10]. Cette injonction désigne pour les États le devoir de perpétuer le souvenir de certains évènements particulièrement graves de l'histoire humaine comme la Shoah, les génocides ou les guerres. Ce devoir a pour fonction, notamment, de rendre honneur aux victimes au travers de l'érection de monument et de la perpétuation de leur souvenir mais aussi de lutter contre la répétition de ces évènements.

Le terme « de devoir de mémoire » est cependant peut-être inapproprié[11]. Nous avons établi lors de notre analyse de l'identité personnelle que la mémoire est un phénomène biologique et subjectif. Au contraire, la mémoire présentée par l'historien est objectivée et reconstruite, c'est donc une « histoire ». Dès lors, il faudrait parler, plutôt que d'un devoir de mémoire, d'un « devoir d'histoire » qui, à la subjectivité et au caractère émotionnel de la mémoire individuel, substitue une forme d'objectivité. Dans la mesure où l'histoire implique la sélection des faits que l'on met en lumière, l'oubli est inhérent à sa mise en œuvre. Néanmoins, cet oubli n'est pas le fait d'un individu mais d'une méthode de recherche et d'analyse de sources et de construction de justifications à ces analyses.

Section 2 - La nécessité de l'oubli dans la condition numérique

Nous avons, dans un premier temps, défini l'oubli et ses relations avec la mémoire. Cette dernière est un élément nécessaire à l'action aussi bien individuelle que politique. Sur le plan social, se souvenir est autant un impératif pratique que moral. On ne peut pas, à ce stade de la réflexion, parler d'un « droit à l'oubli ». La constitution de la mémoire collective passe certes par

---

10 Nous reprenons cette expression à Paul Ricoeur. Voir notamment Ricoeur, P. La mémoire, l'histoire, l'oubli Seuil, 2007, pp. 105-106.

11 Nous reprenons ici notamment les critiques formulées par Ricoeur sans ignorer qu'elles ont donné lieu à de vives réactions.

la sélection d'un ensemble de traces que l'on met en relief, cependant l'oubli est ici plutôt un effet secondaire de cette sélection que ce qui est recherché.

Afin de préciser le sens possible d'un « droit à l'oubli », il ainsi nécessaire de se demander si l'oubli peut et doit être recherché en soi, non pas par exemple à des fins de dissimulation mais pour des raisons intrinsèquement positives. Nous poserons cette question dans le cadre de la « condition numérique ». Les outils informatiques jouent en effet aujourd'hui un rôle primordial dans notre rapport aux autres et à nous-mêmes. Ce sont, pour la plupart, des outils de collecte, de stockage et de diffusion des traces. Si, dans le cadre de revendication de la protection de la vie privée, par exemple, la diffusion et la perte de contrôle des traces est régulièrement décriée, il faut reconnaître que nous cultivons notre visibilité et son enregistrement par exemple en utilisant les réseaux sociaux numériques et plus largement en utilisant des outils informatiques. Nous ouvrirons notre réflexion sur l'analyse de la condition numérique à nous rendre de plus en plus visible ainsi que les débats qui entourent la conservation des traces de cette exposition. Nous élaborerons ensuite une critique de la difficulté de l'oubli dans la condition numérique.

I- Une « morale de la transparence »[12] ?

La visibilité numérique est à la fois issue de l'exposition volontaire des individus sur des plateformes numériques ou en utilisant les services numériques et de l'enregistrement permanent de l'activité des utilisateurs, parfois à leur insu. L'emploi de *cookies* – des fichiers par utilisés par les sites Internet afin de conserver des informations sur leurs utilisateurs – est ainsi l'un des exemples les plus répandus de collecte, souvent sans que les utilisateurs ne le sachent, de traces de navigation[13].

Malgré la crainte des atteintes possibles à la vie privée causées par ces pratiques, il faut noter un apparent désintérêt des utilisateurs pour la collecte de leurs données et le paramétrage de leur visibilité et l'encouragement à l'exposition de soi élaborée par les fournisseurs de services numériques. Ainsi Mark Zuckerberg, par exemple, est-il célèbre pour avoir affirmé l'extension de la visibilité de notre vie et de nos pratiques et avoir débouté les critiques possibles de cette extension. Le PDG de *Facebook* souligne en effet que la visibilité est aujourd'hui un fait. L'utilisation des réseaux sociaux numériques témoigne, pour lui, de la large acceptation de la collecte et de l'utilisation de nos données. Eric Schmidt, qui dirige *Google*, alors que la politique de gestion des données des utilisateurs de son entreprise est violemment critiquée, répond qu'il n'y a rien à craindre de la visibilité et de la conservation des données tant que le sujet des données n'a rien à se reprocher. La visibilité, et la conservation des traces, sont des lors des outils de contrôle social. Ils permettent de maintenir la sécurité – les conditions d'utilisation des sites Internet mentionnent souvent la possibilité de transmettre leurs données aux autorités – ainsi qu'à sa prévention. Dans la mesure où tout est potentiellement enregistré, la visibilité peut avoir un effet

12 La dénonciation d'une « morale de la transparence », c'est-à-dire d'une injonction à se rendre visible, notamment au moyen des outils numériques, fait l'objet de l'ouvrage de Thomas Berns Gouverner sans gouverner. Voir Berns, T. Gouverner sans gouverner ; une archéologie politique de la statistique Presses Universitaires France, 2009

13 La directive européenne 2002/58 sur la vie privée et les communications électroniques, amendée par la directive 2009/136, impose le recueil d'un consentement préalable de l'utilisateur à l'utilisation de cookies lors de sa navigation sur l'Internet.

dissuasif. De plus, dans la mesure où l'enregistrement des traces est facile à automatiser, il constituer un moyen de contrôle social léger, applicable à l'ensemble des utilisateurs et, pour cette raison, efficace.

À la justification factuelle de l'enregistrement de nos traces, Schmidt substitue une justification d'ordre morale. Se rendre visible, ou du moins accepter cette visibilité, est une preuve d'innocence. Bien sûr, on peut opposer à cette position les risques que représentent, pour un individu, l'enregistrement et la conservation de ses traces. La conservation et la diffusion de nos traces, rendues plus faciles par leur numérisation peuvent en effet porter préjudice aux individus. Elles peuvent permettre d'utiliser des informations dans des contextes qui ne sont pas les contextes dans lesquels elles ont été diffusées[14]. Diffuser des informations personnelles sur des sites Internet largement accessible expose ainsi au risque de voir ces informations employées par un public qui n'appartient pas au cercle des intimes. Dans la mesure où les informations sont régulièrement dupliquées, échangées et publiées – soit par des communautés d'utilisateurs, soit par des entreprises dans le cadre de contras commerciaux, ou encore par des institutions – les partager, c'est aussi s'exposer au risque de voir des informations utilisées sans qu'elles soient remises en perspective avec l'époque à laquelle elles ont été collectées.

Néanmoins, la « morale de la transparence », c'est-à-dire l'ensemble des justifications qui concourent à faire de la visibilité de nos pratiques, le plus souvent par leur enregistrement et leur conservation, un phénomène acceptable, voire nécessaire, doit être complétée par un ensemble de justifications d'ordre utilitaristes. L'analyse du « capital social »[15] produit par l'enregistrement et l'utilisation des traces dans le monde numérique permet en effet de souligner que nous tirons de nombreux bénéfices de la visibilité et de l'enregistrement de nos conduites. Parmi ces bénéfices, il faut citer la personnalisation croissante des services que nous utilisons et l'éclosion de nouvelles opportunités de contacts ou d'action. Nous avons cité l'intérêt financier que représentent le stockage et le traitement des données des utilisateurs pour les entreprises privées. Dans le domaine public, le mouvement de l'*Open Data*, c'est-à-dire du partage des données détenues par les pouvoirs publics, est présentée comme un moyen de rendre aux citoyens un bien qui leur appartient et de leur permettre de créer des services à partir de ces dernières. La conservation des données et leur partage est dés lors un outil de maximisation des bénéfices de nos actions.

II- Deux exemples de visibilité exhaustive : le panoptique et la société de contrôle.

Les risques que représentent les usages des traces qui portent potentiellement atteinte aux utilisateurs font douter de l'acceptabilité de la morale de la transparence. Néanmoins, une partie des traces qui sont enregistrées sont anodines, par exemple, parce qu'elles sont purement techniques. Pour autant, la difficulté de l'oubli nous semble propre à instaurer un rapport stratégique entre le sujet décrit par les données et le détenteur de ces dernières. Le sujet des

14 Nous nous inspirons ici de la réflexion d'Helen Nissembaum qui propose d'adopter une définition « contextuelle » de la vie privée. Par contexte, il faut ici entendre un contexte social qui permet de définir les normes de visibilité et d'accès à un ensemble de traces. Voir Nissenbaum, H. Protecting Privacy in an Information Age: The Problem of Privacy in Public Law and Philosophy, Springer, 1998, 17, 559-596.

15 Le « capital social » est l'ensemble des affects positifs produits chez les utilisateurs par les outils numériques. Voir Vallor, S. Social Networking Technology and the Virtues Ethics and Information Technology, 2010, 12, 157-170.

données est en effet exposé au traitement des données par celui qui les stocke. Par analogie, ce rapport nous semble proche de celui que l'on trouve dans le panoptique, une prison imaginée par Jeremy Bentham et étudiée par Michel Foucault et *Surveiller et Punir*[16]. Bentham, en imaginant le panoptique, souhaitait répondre au besoin d'imaginer des prisons qui puissent contenir un grand nombre de prisonniers sans devoir reposer sur un nombre de gardiens trop important. Il s'agissait aussi, pour lui, d'envisager les prisons comme des moyens d'observer et, au besoin, de corriger le comportement des prisonniers. La prison panoptique se présente comme un anneau qui encercle une tour centrale. Dans l'anneau sont logés les prisonniers. Chacun possède sa cellule et chaque cellule est traversée par la lumière : tout ce qui se passe dans la cellule est visible de l'extérieur. Dans la tour se trouvent les gardiens qui peuvent voir ce qui se passe dans les cellules autour d'eux. Les prisonniers ne peuvent jamais savoir si des gardiens se trouvent dans la tour. Un nombre restreint de gardiens est suffisant afin de surveiller l'ensemble des prisonniers.

Sous la plume de Foucault, l'étude du panoptique permet de tirer deux enseignements principaux. Tout d'abord, la visibilité est au fondement d'une stratégie de normalisation des conduites. L'exposition des prisonniers aux gardiens est un moyen de recueillir des données sur les prisonniers et de leur prescrire des exercices pour identifier leur comportement, leurs déficiences et les rééduquer. Foucault remarque d'ailleurs que le rapport de visibilité et force entre le prisonnier et le gardien que l'on trouve dans le panoptique était d'ailleurs conçu par Bentham comme pouvant s'étendre à d'autres bâtiments comme les prisons ou les hôpitaux. Foucault nomme ce phénomène « discipline ».

Ensuite, le rapport qui se noue entre les gardiens et les prisonniers participe à la constitution des comportements des prisonniers et, *in fine*, à la création de leur subjectivité. Dans la mesure où les prisonniers ne savent jamais s'ils sont effectivement observés, ils doivent se conduire comme si tel était le cas. La possibilité même de la visibilité crée donc le sentiment de l'observation permanente et un ensemble de conduites qui prennent appui sur ce sentiment. L'exemple du panoptique fournit ainsi un cas dans lequel la visibilité apparaît comme un moyen de contrôle social efficace qui transforme la subjectivité des individus auxquels il s'applique. Il rappelle aussi que, dans le cas du panoptique, la visibilité assujettit les prisonniers.

La condition numérique repose sur la séparation entre les possesseurs de données – les entreprises privées ou les institutions par exemple – et les sujets décrits par ces données. Souvent, l'accès aux données est complexe et seuls les possesseurs des données peuvent les traiter. Nous sommes ainsi face à une forte asymétrie de la visibilité des utilisateurs. Tout comme le gardien agit sur le prisonnier à partir de l'observation qu'il en fait, les possesseurs des données agissent sur les utilisateurs, par exemple au moyen du « marketing des traces »[17], qui consiste à utiliser les traces des sujets des données dans des stratégies publicitaires.

Néanmoins, alors que les prisonniers du panoptique sont séparés les uns des autres puisqu'ils sont dans des cellules et qu'ils ne peuvent se déplacer librement, dans le cas du développement des outils numériques, le déplacement est facilité grâce aux outils mobiles et la

16 Voir Bentham, J. Le Panoptique P. Belfond, 1977 et Foucault, M. Surveiller et punir Gallimard, 1993.
17 Voir Kessous, E. L'attention au monde Armand Collin, 2012, p. 59 et sq.

communication est aisée, voire encouragée. Il faut ainsi amender le modèle du panoptique, par exemple à la manière de Gilles Deleuze lorsqu'il décrit la « société de contrôle »[18].

Alors que les bâtiments auxquels la discipline s'applique ont chacun une fonction bien définie, la visibilité numérique s'étend à toutes les aires de notre vie. Nous sommes visibles non seulement à celui qui fournit les moyens de communication (par exemple un réseau social numérique), mais aussi à tous les gens avec qui nous communiquons et, comme le montre les récentes révélations d'Edward Snowden, par ceux qui peuvent accéder de manière autorisée ou non, à ces communications. On ajoute ainsi à la « surveillance », une observation motivée par le risque que représentent une personne ou un groupe, une forme d'observation permanente des utilisateurs entre eux, avec les dangers que l'on connaît bien en termes de discrimination par changement de contexte des traces.

Alors que l'architecture du panoptique est figée, la « société de contrôle » repose ainsi sur un cadre souple et qui s'adapte à nos pratiques. De plus, alors que le rapport disciplinaire est de l'ordre de la coercition, Deleuze note que le cadre du contrôle est souvent ludique et qu'il est présenté comme augmentant notre sécurité et nos possibilités d'action. Néanmoins, pour l'auteur, tel n'est pas le cas. Alors qu'il est possible de s'échapper de la prison panoptique, il est impossible de « sortir » de la société de contrôle puisqu'il n'y a pas d'extérieur du système. Pour Deleuze, on passe de la « discipline » au « contrôle » : alors que la discipline « rééduque » les prisonniers, les ouvriers ou les écoliers, le contrôle prend appui sur la « réalité » qu'elle cherche à influencer et à programmer, par le biais d'un « marketing des traces » qui se découpe en deux étapes. Premièrement, la collecte des traces la plus exhaustive possible est nécessaire afin de constituer une base de connaissances. Ensuite, l'analyse de la base obtenue, le plus souvent au moyen d'outils statistiques permet de modéliser les phénomènes décrits par les données. Le contrôle est ainsi un pouvoir « bienveillant » puisqu'il a une prétention à se fonder sur la « réalité » qu'il s'agit, en quelque sorte, de programmer[19]. Une telle argumentation passe sous silence les effets sur la subjectivité des individus des stratégies de contrôle.

Or, c'est ici que se loge l'une des difficultés de ce pouvoir. Il donne à voir notre monde comme un « tout » dans lequel toutes les vies sont enchevêtrées. Les histoires personnelles et les interactions sociales s'imbriquent ainsi pour former un système, c'est-à-dire un ensemble clos d'éléments interdépendants, analysés à l'aide des outils statistiques. Pourtant, la constitution d'un gouvernement que l'on peut dire « algorithmique » avec Thomas Berns et Antoinette Rouveroy, dans la mesure où l'analyse des conduites et l'utilisation de ces analyses sont réalisées par des algorithmes ce qui en facilite l'automatisation, se heurte à deux écueils.

Tout d'abord, nous avons rappelé que nous étions des « animaux autobiographiques »[20] puisque notre identité prend la forme d'une narration. Il est difficile d'élaborer une telle narration dans le monde numérique où le temps est représenté non pas du point de vue de son

---

18 Deleuze G., « Post-scriptum sur les sociétés de contrôle » in Pourparler, Paris, Éditions de Minuit, 2003.

19 La dénonciation de ces traits fait l'objet du travail d'Antoinette Rouveroy. Voir notamment Rouveroy, A. « Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation? », Politique des algorithmes. Les métriques du web. Reseaux, Vol.31, n.177, pp. 163-196, 2013.

20 Nous reprenons ici le titre d'un colloque consacré à Jacques Derrida. Voir Mallet, M.-L. L'animal Autobiographique Galilée, 1999.

déroulement de sa prévisibilité. De plus, la narration d'une autobiographie s'appuie sur l'énoncé de valeurs qui guident nos acteurs. C'est dans cette mesure que les actes peuvent être considérés comme intentionnels. Nous avons des projets, nous visons des fins et nous raisonnons en fonction de valeurs, autant d'éléments que nous pouvons relater. Le gouvernement inadéquat est, sous cet angle, inadéquat. Nous ne « programmons » par nos vies à la manière d'un algorithme, d'où le conflit entre deux manières de décrire notre monde[21].

Ensuite, le système présenté par la société de contrôle est clos. Il forme une « totalité »[22]. Pourtant, l'Histoire humaine est faite de ruptures, par exemple dans le savoir et les techniques qui modifient radicalement ce que nous pouvons faire ou dire et la manière dont nous interprétons nos vies. Dès lors, une biographie et les évaluations que l'on peut former ne sont jamais figées. Dès lors, à la morale de la transparence et l'enregistrement permanent de nos traces, il faut opposer la nécessité du pardon et du recommencement. Le pardon ne consiste pas à effacer effectivement un fait mais à faire comme s'il ne s'était rien passé, c'est-à-dire à l'oublier. En quelque sorte, pardonner consiste à réécrire une histoire. Dans cette perspective l'oubli est nécessaire dans le cadre de la condition numérique. Le détour par le pardon permet de définir le droit à l'oubli comme la prérogative d'un individu qui peut contrôler la conservation de traces qui le concernent.

Section 3 - Les formes de l'oubli numériques[23]

L'analyse du pardon et des effets de la visibilité permanente et de la conservation des traces permet d'établir la nécessité de l'oubli pour le maintien de la vie sociale. Néanmoins, face à l'engouement pour les services numériques mais aussi à l'architecture de ces derniers qui est orientée vers la conservation des traces, il faut désormais s'interroger sur la possibilité pratique de l'oubli et les mécanismes qui le permettraient. Nous avons souligné la parenté entre le droit à la vie privée et le droit à l'oubli. Ce dernier met moins l'accent sur la nécessité d'identifier des données personnelles ou intimes et plus sur la capacité des sujets des données à contrôler la conservation de leurs traces. Nous proposons, pour penser la mise en œuvre du droit à l'oubli, de repartir des mises en œuvre du droit à la vie privée.

On peut tout d'abord, dans le cas d'un « droit à l'oubli », envisager l'oubli comme le résultat d'une demande, effectuée par exemple par un individu concerné par un ensemble de traces. Dans ce cas, l'oubli est le résultat d'une contractualisation : l'utilisateur d'un service doit être informé des données le concernant que le service possède. Il doit aussi être informé des moyens d'accès et de modification de ces données qu'il possède. La loi Informatique et Libertés de 1978, par exemple, ne garantit pas explicitement un droit à l'oubli. Néanmoins, cette loi garantit un droit de rectification des données. L'exercice de ce droit repose sur l'initiative des

---

21 Nous reprenons ici la distinction entre programmation et intention que l'on trouve dans l'éthique de la vertu et notamment chez A. MacIntyre. Voir MacIntyre, A. After Virtue: A Study in Moral Theory University of Notre Dame Press, 1984.

22 Nous reprenons ici le vocabulaire d'E. Levinas. Voir Levinas, E. Totalite et Infini Springer, 1984

23 Cette dernière partie est inspirée par l'ouvrage d'E. Kessous. Voir ibidem.

sujets des données qui doivent accomplir les démarches nécessaires auprès des possesseurs de données ou bien de médiateurs à même de demander la rectification des données.

On peut aussi, dans le cas où on considère l'oubli comme une nécessité sociale, envisager, de la part des possesseurs de données, un « devoir d'oubli ». Dès lors, la responsabilité de l'oubli incombe au possesseur des données, chargé de veiller à l'effacement des données qu'il enregistre. Aujourd'hui, les politiques de conservation des données des moteurs de recherche permettent d'envisager un exemple de mise en œuvre de l'oubli par les possesseurs de données. *Google*, par exemple, anonymise les données recueillies par son moteur de recherche au bout de neuf mois puis les efface.

Du point de vue pratique, les deux approches reposent sur un voisinage conceptuel et des solutions techniques distinctes. Le « droit à l'oubli » met l'accent sur la responsabilité de celui qui est concerné par un ensemble de traces. Il est lié à une conception des traces comme la propriété de celui qu'elles concernent. Ce dernier doit dès lors consentir à leur collecte puis, lorsqu'il souhaite y accéder ou les faire rectifier, l'exprimer de manière explicite. Néanmoins cette conception se heurte à la difficulté de déterminer la portée du consentement numérique.Sur l'Internet, par exemple, les utilisateurs doivent accepter des conditions d'utilisation afin d'accéder à un service. Il en est de même pour les logiciels. Ces conditions précisent notamment les données collectées et les politiques de traitement de ces dernières. Les entreprises comme *Google* mettent en outre une documentation importante sur cette politique. Néanmoins, le plus souvent ces conditions ne sont pas lues parce qu'elles sont trop longues, peu lisibles et que le service est souvent jugé comme « nécessaire » ou suffisamment pratique pour accepter un sacrifice. Enfin, elles sont parfois peu compréhensibles pour les utilisateurs. L'étape de consentement, qui est pourtant cruciale dans le cas où l'accent est mis sur l'autonomie de l'individu décrit par les traces, est ainsi souvent réduite à un automatisme nécessaire pour profiter d'un service numérique.

Néanmoins, l'utilisation de nombreux services numériques, comme les sites Internet, ne reposent pas sur l'acceptation de conditions d'utilisation des données. Dès lors, certains sites tiennent compte des réglages du navigateur des utilisateurs pour déterminer ses préférences en termes de collecte de données. Même dans les cas où l'utilisateur accepte la collecte des données, par exemple au moyen de *cookies*, le consentement ne résout pas l'ensemble des questions pratiques soulevées par la collecte et le stockage des données. Lorsqu'un site reconnaît utiliser des données, il ne précise ainsi pas qui a accès aux *cookies* ni s'il héberge des *cookies* élaborées par des entreprises tierces. Il ne précise pas non plus la durée de conservation des données qu'ils décrivent et comment sont-elles traitées.

Enfin, la mise en œuvre du droit à l'oubli se heurte à la difficulté d'identifier les données qu'il faudrait rectifier ou effacer. Le critère des données « personnelles », par exemple, n'est pas satisfaisant s'il se limite aux données qui identifient un sujet déterminé puisque le large éventail des données disponibles permet, par recoupement, d'inférer des données personnelles. La mise en œuvre du « droit à l'oubli » se heurte ainsi à un éventail de difficultés pratiques De plus, la diversité des législations auxquels les possesseurs de données sont soumis et l'apparent désintérêt des utilisateurs pour les mécanismes comparables mis en œuvre dans la protection de la vie privée conduisent à douter de leur efficacité.

Par « devoir d'oubli » il faut entendre l'automatisation et la systématisation de l'oubli en créant une obligation pour celui qui possède des données de les effacer. Bien sûr, l'effectivité des

règles de droit sur des compagnies qui ont des sièges dans des états différents reste un problème ouvert. Néanmoins, l'exemple de la limitation des durées de conservation par les industriels, semble ouvrir une voie proposée, par exemple par Emmanuel Kessous[24]. Dans son analyse de la vie numérique et de la protection de la vie privée, Kessous note que la définition de normes – comme les normes européennes – permettent d'associer les industriels à la réflexion et la mise en pratique de la protection des utilisateurs selon des moyens qui se révèlent efficaces.

Conclusion

Nous avons commencé notre réflexion par la définition de l'oubli au mieux comme un fait avec lequel il faut vivre, au pire comme une perte contre laquelle il faut luter. Les outils numériques constituent des moyens de luter contre une telle perte. Néanmoins, la condition numérique crée une situation dans laquelle il est complexe de rester maître de la narration de sa biographie. C'est afin de restaurer une telle capacité que l'oubli peut prendre une signification positive. Résultat d'une sélection et d'une mise en forme des traces qui nous concernent, l'oubli est un moyen de reprendre possession des traces que nous laissons. C'est pour cette raison que, malgré les difficultés pratiques auxquelles se heurtent sa mise en œuvre l'oubli nous semble être devenu un droit. Le terme oubli ne doit d'ailleurs pas être réduit à un synonyme d'effacement, notre analyse permettant d'établir que l'oubli peut passer non seulement par la suppression des traces mais aussi leur modification ou leur anonymisation par exemple.

24 Ibidem, p. 129 et sq.

DEUXIEME PARTIE

Le Droit à l'oubli,

Affirmation et manifestations

CHAPITRE 1

Droit à l'oubli numérique,

la loi informatique et libertés et le projet de règlement européen[1]

1. Evolution de l'internet. L'Internet existe déjà depuis quelques décennies mais les évolutions intervenues ces dernières années, dans le domaine des technologies de l'information et de la communication génèrent des changements considérables. La diversité des applications de l'Internet a certes contribué à ce qu'il se taille un succès imposant auprès du public, hissant en quelques années l'Internet « au rang de phénomène socioculturel majeur »[2], cette diversité a également engendré la multiplication des fichiers et des traitements automatisés hissant, sous cet angle là, l'Internet « au rang d'espace liberticide totalement débridée ».

2. L'Internet soumis au droit. Mais l'Internet en vertu de son universalisme et de ses caractères spontané et immatériel, serait-il un lieu réfractaire à l'emprise du droit ? La réponse paraît évidente, l'Internet doit être encadré par le droit, encadrement qui se justifie d'autant plus que « la nouveauté est que les intérêts ici en conflit le sont à l'échelle mondiale, que leurs enjeux sont colossaux en termes de puissance, de richesse et d'emplois et qu'il touche à l'être autant qu'à l'avoir puisqu'ils intéressent l'intimité et le savoir des personnes »[3]. Si l'on vient de répondre à la question de savoir si l'Internet, doit ou non, rester « aux portes du droit », encore faut-il déterminer à quel(s) droit(s) l'on doit le soumettre ? En effet, si la technique est nouvelle - en tout cas à l'échelle du droit - nombre de questions juridiques fondamentales qu'elle fait naitre sont intemporelles. Ainsi, suffit-il au prix de quelques adaptations, soumettre l'Internet aux droits nationaux et internationaux existants ou est-il nécessaire de lui appliquer des règles qui lui sont propres ?

3. L'adaptation du droit à l'Internet. A cette question le législateur a peu à peu opté pour la deuxième solution, sans pour autant totalement écarter la compétence du droit commun. Ainsi, même après l'adoption de la loi sur l'informatique, les fichiers et les libertés du 6 janvier 1978, dite Loi Informatique et Libertés (LIL), règlementant - tant bien que mal - la collecte et l'utilisation des informations dites « nominatives », qui permettent d'identifier, directement ou indirectement, des personnes physiques, le droit commun au travers de l'article 9 du Code Civil[4]

---

1 Par Latifa Chelbi, Attachée temporaire d'enseignement et de recherche à la Faculté de droit de Grenoble

2 L.Cohen-Tangui, Le nouvel ordre numérique, In: Réseaux, Odile Jacob 1999, P.172.

3 P.Catala, « Actualité du droit de l'Internet », CCE juin 2003, Repères, P.3

4 Article 9 du Code Civil qui dispose que : « Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.»

par exemple, orchestré par la jurisprudence, n'a t-il pas vocation à remplir son office sur l'Internet comme si de rien était.[5] Quelles que soient les conditions de l'intervention du droit, celle-ci est d'autant plus nécessaire dans la mesure où même si les questions juridiques que suscite l'Internet sont intemporelles, il n'en reste pas moins qu'elles doivent être réexaminées sous une nouvelle approche répondant aux nouveaux enjeux liés aux technologies de l'information et de la communication.

4. La protection « inadaptée » de l'internaute par le droit au respect de la vie privée. En effet, la circulation d'information sur les supports de communication numérique est facilitée et instantanée. Le nombre d'information et de données personnelles publiées chaque jour est croissant. A chaque connexion l'internaute sème des traces conscientes (login, mot de passe etc.) ou inconscientes (via les aspects de gestion technique tel que les cookies[6] par exemple) sur les réseaux sociaux et professionnels, les blogs ou encore les sites marchands. Ces informations sont collectées et stockées à l'insu[7] de la personne concernée et c'est pourquoi il est aisé dans notre cyber-société de porter atteinte à la vie privée des internautes, car il est aisé de détourner ces informations de leur finalité première. À l'égard des risques sus évoqués par le traitement des données personnelles, le législateur s'est interrogé sur le point de savoir si la protection de la vie privée apportait des garanties suffisantes. Les limites d'une protection des informations personnelles par le droit au respect de la vie privée sont rapidement montrées du doigt[8]. Elles tiennent notamment au caractère restrictif de la notion de vie privée, les auteurs considérant en effet, que l'article 9 du Code Civil est « une disposition générale insuffisante pour protéger contre les risques que représente pour les libertés individuelles le traitement informatisé des données nominatives[9] » ce qui justifie que l'on s'oriente vers un autre système de protection à savoir le droit à la protection des données à caractère personnel[10].

5. La protection de l'internaute par la protection de ses données à caractère personnel. Cette notion, excluant la prise en compte du contenu de la donnée, ce qui conditionne pour le régime de droit commun la prise du droit au respect de la vie privée, s'attache quant à elle à la nature de la donnée[11]. Si la nature de la donnée permet de déterminer le

---

5 TGI Paris 17ème chambre, 6 novembre 2013 Max M. /Google France, Google Inc : « Attendu que, contrairement à ce qu'affirme la société défenderesse, le droit français prévoit, notamment dans l'article 9 du code civil, la possibilité pour les juges de "prescrire toutes mesures, (...) »

6 Il s'agit de fichier émis par le site que l'internaute consulte qui, une fois enregistré sur le disque dur de l'ordinateur, permet l'identification de l'ordinateur lors de nouvelles connexions.

7 Démonstration du traçage numérique sur le site de la CNIL : « Comment vous êtes pisté ? » http://www.cnil.fr/vos-droits/vos-traces/

8 Notamment par la commission en charge de la préparation de Loi Informatique Et Libertés : Commission informatique et libertés, Rapport Tricot, La Documentation française, 1975, tome 1, p. 19.

9 I.de Lamberterie, Informatique, Libertés et opinions religieuses, Archives des sciences sociales des religions, 1995, Volume 91, n°1, P.21-39

10 Notion plus « englobante » car ne se limitant pas aux seules informations relatives à la vie privée et définit comme toutes informations se rapportant à une personne physique identifié ou identifiable, indépendamment du caractère intime ou privée de la donnée.

11 Mme de Lamberterie et M. Lucas, « pour être relative à la vie privée, une information doit concerner la vie personnelle et familiale ; elle est qualifiée par son contenu. Pour être personnelle, une information doit seulement

caractère personnel de celle-ci, l'on a du également retenir le critère du temps - en vertu du caractère définitif que revêt la conservation des données sur l'Internet - afin de donner prise à la protection.

6. Le droit à l'oubli numérique. La question du « droit à l'oubli numérique », lequel permettrait à toute personne de demander au site publiant des données à caractère personnel la concernant d'en obtenir le retrait après l'écoulement d'un certain laps de temps, est alors venue animer les débats, tant au niveau national, international qu'européen. Les faiblesses et l'inadaptation du droit commun appliqué au support numérique ont poussé le législateur à intervenir en adoptant la Loi Informatique et Libertés instaurant ainsi les prémices d'un droit à l'oubli numérique (I) ; droit à l'oubli numérique qui reste à consacrer à travers, notamment, le projet de règlement européen (II).

Section 1 - La Loi Informatique et Liberté ou les prémices du droit à l'oubli numérique.

7. Adoption de la LIL. En se dotant d'une loi relative à l'informatique, aux fichiers et aux libertés, la France a été l'un des premiers pays à percevoir les dangers résultant pour les libertés des citoyens du développement de l'informatique et, en conséquence, à encadrer la collecte et le traitement des données. Dès 1971, le Conseil d'État adressa au Gouvernement, une recommandation visant à encadrer l'usage des données personnelles. Mais la prise de conscience des enjeux liés à cette question intervint en 1974, face à un projet gouvernemental connu sous le nom de SAFARI[12]. Ce dispositif suscita alors de fortes réactions[13], à la suite de quoi le projet fut retiré et une commission chargée de proposer des mesures tendant à concilier le développement de l'informatique dans les secteurs public, semi-public, privé et le respect de la vie privée, crée. Le rapport issu des travaux de la commission, rédigé par M. Bernard Tricot et M. Pierre Catala, remis en juin 1975, a inspiré le projet de loi relatif à l'informatique, aux fichiers et aux libertés ; loi n° 78-17 qui sera finalement adoptée le 6 janvier 1978. La Commission Nationale Informatique et Libertés (CNIL), autorité administrative indépendante, sera également crée. Cette loi a été modifiée à plusieurs reprises et substantiellement par la loi du 6 août 2004 qui transpose en droit français les dispositions des directives n° 95/46/CE 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 n°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. Mais également par la Loi n° 2011-334 du 29 mars 2011 relative aux défenseurs des droits et dernièrement par la Loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique modifiant l'article 13[14] de la loi.

être rattachée à une personne ; elle est qualifiée par sa nature. Il apparaît alors clairement que les données personnelles excèdent largement la catégorie des informations relatives à la vie privée.

12 « Système automatisé des fichiers administratifs et du répertoire des individus », qui prévoyait une interconnexion des fichiers publics à partir d'un identifiant unique, à savoir le numéro de sécurité sociale

13 http://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg « La chasse aux hommes » Le monde 21/03/1974

14 Article concernant la CNIL

8. Cadre juridique instauré par la LIL. Cette loi institue ainsi un cadre pour le traitement des données à caractère personnel et réglemente, dans ses dispositions initiales, la collecte et l'utilisation des dites données. Données à caractère personnel que l'on définit comme toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou par rapport à des éléments « propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale » .Les contours de cette définition légale ont été précisés par la jurisprudence tant administrative que judiciaire notamment en matière de sondage (Affaire Syntec et Sofres)[15]. Si l'on vient de définir la notion même de donnée à caractère personnel, encore faut-il envisager le champ d'application de la protection. Ainsi, pour pouvoir prétendre à la protection conférée par la Loi Informatique et Libertés, les données doivent concerner une personne physique. En effet, la loi de 1978 vise directement la personne physique : « Constitue une donnée à caractère personnel toute information relative à une personne physique... », sont donc clairement exclut de son champ d'application les personnes morales[16], elle vise le citoyen, autrement dit, tout « internaute potentiel ». Mais les données doivent également faire l'objet d'un traitement automatisé ou non c'est-à-dire « 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 »[17]. Une fois ces éléments réunis « une série de droits séparés mais formant une chaîne fonctionnelle de droit intégrés[18] » est alors octroyée à l'internaute « fiché ». En effet, contrairement à d'autres droits de la personnalité (comme le droit au respect de la vie privée) se contentant d'énoncer le droit sans préciser le contenu, la Loi Informatique et Libertés énumère précisément le contenu des droits conférés à l'internaute comme suit :

- Un droit à la loyauté de la collecte[19] ou un droit à consentir : la collecte doit avoir été consentie pour ne pas être déloyale. Le cas des cookies illustre le problème. Ils doivent être implantés avec l'accord de la personne concernée à défaut, il y a collecte déloyale d'informations directement ou indirectement nominatives, ainsi qu'une intrusion dans un système informatique qui peuvent être pénalement répréhensibles[20].
- Un droit d'accès et de rectification[21] : Le premier permet de savoir si les données concernées sont toujours traitées, obtenir leur communication et connaître « la

---

15 Conseil d'Etat 9 Juillet 1997, Affaire Syntec et Cour de Cassation, Chambre criminelle 12 Mai 1998, Affaire Sofres, n° 96-85.900 : « Les résultats d'un sondage portant sur une personne, qui représentent l'état statistique, à un moment donné, de l'opinion de la population sur celle-ci, ne constituent pas une information nominative au sens de l'article 4 de la loi du 6 janvier 1978. Il s'en déduit que, dès lors que les résultats ne lui sont pas opposés, cette personne ne saurait bénéficier du droit d'accès et des prérogatives qui en découlent, prévus par les articles 34 et suivants de ladite loi, ni exiger la communication du nom du commanditaire de l'opération. »

16 Lire à ce sujet la contribution de Mme Amélie FAVREAU, Maitre de conférences en droit privé

17 Article 2 de la loi

18 Lucas (A.), Deveze (J.), J. Frayssinet (J.), Droit de l'informatique et de l'Internet, PUF, Paris, 2001

19 Article 6 de la Loi Informatique et Libertés : « Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : 1° Les données sont collectées et traitées de manière loyale et licite »

20 Cassation criminelle, 14 mars 2006, n°pourvoi : 05-83423 : Bull. crim. 2006, n°69, http://legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007069872

21 Article 39 de la Loi Informatique et Libertés : « Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : 1° La confirmation

logique qui sous-tend le traitement ». C'est ce que le Professeur J.Frayssinet nomme *le droit à la curiosité*. Le second permet de rectifier les mentions inexactes, ou dont le traitement est interdit et selon les cas en demander l'effacement avec la notification aux tiers de toute rectification ou suppression éventuelle.

- Un droit d'opposition : toute personne physique peut s'opposer, pour des raisons « légitimes », à ce que des informations nominatives la concernant fassent l'objet d'un traitement, à l'exclusion de ceux qui sont mis en œuvre par les autorités publiques ou par les personnes privées gérant un service public. La notion de raisons légitimes n'étant pas définie, on peut supposer que l'on a le droit de s'opposer à tout traitement qui va à l'encontre de l'esprit de la loi (article 1er) ou qui enfreint une quelconque disposition de celle-ci. La modification opérée par la transposition de la directive va au delà du simple droit d'opposition en consacrant le principe du consentement indubitable de la personne concernée par le traitement.[22]Il en résulte que le responsable de traitement doit rechercher positivement le consentement de la personne concernée[23]. C'est pourquoi l'on assimile souvent le droit d'opposition au droit de consentir prévu à l'article 7 de la Loi Informatique et Libertés[24].
- Un droit à l'information : Pour la validité du consentement, l'article 32 de la Loi Informatique et Libertés énonce un droit à l'information portant sur l'identité du responsable du traitement, la finalité de ce dernier et les moyens dont dispose l'internaute pour s'y opposer.

9. Prémices du droit à l'oubli numérique. A ces droits s'ajoute le fait que tout traitement doit être limité dans le temps. En analysant l'article 6 alinéa 5 de la loi de 1978 l'on y trouve une forme diminuée du « droit à l'oubli numérique » (« Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : [...]5° Elles sont conservées 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

---

que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ; [...] 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; .. »

Article 40 de la Loi Informatique et Libertés : « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. »

22 C'est à la suite de cette modification que certains auteurs ont très justement remarqué que l'on est passé d'un système « d'opt out » ; système qui désigne le fait de devoir agir par une action positive afin de « retirer son consentement », consentement qui a été préétabli par des paramètres par défaut ; à un système « d'opt-in ou de consentement préalable». Cette même mutation est intervenue en matière de vente à distance : le Code de la consommation retenait le système de l'opt-out, puis la directive du 12 juillet 2002 Vie privée et commerce électronique imposa le consentement préalable en matière de prospection par voie électronique et de vente à distance.

23 Bénéjat (M.) "Les droits sur les données personnelles", in Les droits de la personnalité, sous la direction de J.-Ch. Saint Pau, Lexis-Nexis, 2013: Mais « le système de l'opposition réapparaît après le décès de l'individu puisque « les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit. »

24 Article 7 Loi Informatique et Libertés : «Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée [...]»

traitées. »). Dans sa formulation, cet article transpose le principe de proportionnalité[25] en droit des données à caractère personnel. Ce principe exige ainsi que les données collectées permettant d'identifier directement ou indirectement un individu, ne soient pas conservées *ad vitam aeternam* pendant une durée excessive au regard de la finalité initiale de la collecte. En clair, il s'agit de détruire les données concernant l'internaute dès que leur conservation n'a plus aucun rapport avec la raison initiale ayant justifié la collecte. Il faut donc que la conservation des données soit proportionnelle à ce qui a justifié au départ qu'elles soient collectées puis traitées. Ainsi, l'utilisation licite de toute information personnelle devient illicite par l'écoulement du temps. A défaut de précision législative, la durée nécessaire est laissée à l'appréciation de la CNIL et des juges. Le fait de conserver des données à caractère personnel au-delà de la durée autorisée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende[26]. Plusieurs critères d'appréciation entrent en jeu : l'âge des personnes concernées[27], la nature de la donnée ou encore la finalité du traitement. Ainsi, sans consacrer un véritable droit à l'oubli autonome la Loi Informatique et Liberté en évoque tout de même certains aspects.

10. Limites et fragilités de la LIL. Ces prérogatives que consacre la Loi Informatique et Libertés et qui permettent à l'internaute d'avoir le contrôle et la maitrise de « son soi numérique », tant à priori pour accepter ou refuser le traitement de ses données, qu'à posteriori pour vérifier, rectifier ou supprimer ses données, se heurtent à de nombreuses exceptions et/ou imperfections. Faute de pouvoir être exhaustive, en voici quelques illustrations. Ainsi, l'exercice du droit d'opposition est conditionné à l'existence d'un « motif légitime » alors qu'aucune précision n'est apportée par le législateur quant à ce que l'on doit entendre par la notion de « motifs légitimes ». La personne concernée ne risque-t-elle pas de se heurter systématiquement à la contestation de la légitimité de son motif par le responsable du traitement ? Le droit d'accès est lui aussi soumis à quelques exceptions. Sans citer l'abus de droit[28] inhérent à l'exercice de tout droit subjectif, il n'est pas possible d'invoquer un droit d'accès lorsque les données à caractère personnel sont conservées sous une forme excluant tout risque d'atteinte à la vie privée et pendant une durée limitée, n'excédant pas celle nécessaire aux seules finalités d'établissement de statistique ou de recherche scientifique ou historique. Outre la rédaction large que l'on peut reprocher à cette exception certains auteurs déplorent « un retour en arrière », en effet, l'appréciation de cette dérogation se fera non pas au regard de la nature « plus ou moins personnelle de la donnée » mais au regard de la nature plus ou moins « intime/privée » de la donnée[29].Une autre limite, source d'insécurité juridique, peut également être évoquée. Elle tient au champ d'application matériel de la Loi Informatique et Libertés, en effet ne sont pas soumises à la loi les opérations de

25 Principe de proportionnalité déjà connu en droit administratif par exemple

26 Article 226-20 du Code Pénal

27 Preuve en est du Rapport 2012 consacré aux droits de l'enfant : Enfants et écrans grandir dans le monde numérique.

28 Article 39 II, al.1 Loi Informatique et Libertés

29 « Le retour en arrière » est sans doute justifié par la nécessaire conciliation du droit à la protection des données à caractère personnel avec d'autres droits et libertés fondamentaux. Cf. Notamment la contribution de Mme Julie Aroyo, Doctorante en droit Public.

« caching[30] » et de transit. Quel est alors le sort des données temporairement stockées ou en transit ? L'absence de solution juridique permettant l'effectivité de ces droits, l'insuffisance de moyens dont dispose la CNIL ou l'émergence de nouvelles applications numériques telle que le Cloud Computing, auxquelles la Loi Informatique et Libertés ne s'était pas préparée, sont autant d'autres exemples qui viennent confirmer la nécessaire évolution du cadre juridique actuel en matière de protection des données à caractère personnel. Le droit à l'oubli et plus largement le droit à la protection des données à caractère personnel circonscrit au territoire national aurait incontestablement une portée et une effectivité limitée au vu du caractère transfrontière de l'Internet. La Loi Informatique et Libertés était donc une bonne initiative réactionnaire face à l'émergence d'atteinte à l'identité numérique mais n'avait vocation qu'à contrôler les dérives de l'informatique et n'avait pas appréhendé l'émergence de nouveaux réseaux et le problème de l'accessibilité d'une information personnelle à la planète entière. Les apports et les modifications consécutifs à la transposition de la directive de 1995, quand bien même ils intègrent des avancées intéressantes, telles que la notion de données personnelles, des précisions textuelles par la définition de nombreuses notions (fichiers, traitement automatisé, responsable de traitement), la mise en exergue du consentement, le renforcement de l'obligation d'information et une relative harmonisation entre les Etats membres, restent insuffisants. En effet, la perception des atteintes au droit des personnes peut différer d'un pays à l'autre. Ce qui explique, entre autre, l'inadaptation d'une directive pour régler des enjeux qui se doivent d'avoir des réponses uniformes. Ainsi, l'essence même de la directive en compromet l'effectivité puisque par définition cette dernière lie les États destinataires quant à l'objectif à atteindre, mais leur laisse le choix des moyens et de la forme pour atteindre cet objectif, ce qui favorise une disparité au sein des régimes juridiques des différents Etats Européens ; traduisant une certaine insécurité juridique en cas de transferts de données vers un Etat membre par exemple ou encourageant la pratique du « *regulatum shopping* » incitant les entreprises à s'implanter dans un pays peu regardant des questions relatives à la protection des données à caractère personnel. Mais l'internet ne se cantonne pas aux frontières de l'Europe. Partant, l'on doit avoir une vision internationale, « extra-européenne » de la question d'autant plus que les « maitres » de l'Internet sont Américains. L'article 5 de la Loi Informatique et Libertés précise son champ d'application territorial en énonçant que :

« Sont soumis à la présente loi les traitements de données à caractère personnel :

1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;

2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat 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 Etat membre de la Communauté européenne.[...]

---

30 Ou copie temporaire, vise notamment le recours, par des fournisseurs d'accès, au service « proxy » qui mémorise temporairement les pages visitées par les internautes afin qu'il ne soit pas nécessaire d'accéder au serveur initial en cas de nouvelle requête.

Ainsi, la Loi Informatique et Libertés soumet à son application les traitements dont le responsable est établi[31] sur le territoire français, c'est-à-dire lorsqu'il y exerce une activité réelle et effective au moyen d'implantations stables ou lorsque sans y être établi, il recourt à des moyens de traitements qui y sont situés. Qu'en est-il alors lorsque le responsable de traitement est établi hors de l'Union européenne ? Quand bien même le critère du « recours à des moyens de traitement situés sur le territoire français » semble attractif, le juge français[32], dans les rares décisions relatives à la détermination de la loi applicable en matière de protection des données personnelles, semble réticent à appliquer la Loi Informatique et Libertés pour des atteintes imputables à des responsables de traitement situés hors de l'Union européenne. Les règles classiques du droit international privé trouvent alors à s'appliquer, ainsi, en vertu de la règle *lex loci delicti* l'on retiendra la loi du lieu de la « commission du fait dommageable »[33].

Il est à noter que si la loi prévoit une « limitation géographique » à la protection des données personnelles, elle n'en prévoit pas pour la protection de la vie privée[34]. La directive n°95/46 « ne préjugeant pas des règles de territorialité applicables en matière de droit pénal »[35], il va sans dire

---

31 La notion d'établissement devra s'entendre à la lumière de la jurisprudence de la CJUE notamment affaire Factortame 25 juillet 1991 : « la notion d'établissement, au sens des articles 52 et suivants du traité, comporte l'exercice effectif d'une activité économique au moyen d'une installation stable dans un autre Etat membre pour une durée indéterminée » http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61989CJ0221:FR:PDF

32 TGI Paris, 14 avril 2008 http://juriscom.net/wp-content/documents/tgiparis20080414.pdf , n°08/52010, note J. Lacker, Google sage comme une image ? Ou l'application du droit américain à un site à destination du public français : RLDJ oct. 2008, n°42, P.19. En l'espèce, une personne souhaitait qu'il soit fait obligation à Google de supprimer de ses archives, des messages postés par elle sur des forums de discussion. Elle se fondait pour cela sur la LIL. Le tribunal a estimé que cette loi n'était pas applicable. En effet, les serveurs Google (y compris Google.fr) sont installés en Californie et sont exploités par la société Google.Inc ; la société Google.fr n'étant qu'un responsable commercial et non le responsable du traitement, c'es le droit Californien qui devra s'appliquer.

Vers un revirement jurisprudentiel ? Deux jugements semblent au rebours de cette constante jurisprudence. En effet, dans un premier jugement du TGI de Montpellier en date du 28 octobre 2010 le tribunal, saisi d'une demande de désindexation de contenu litigieux, retient que la LIL est applicable à Google. Cependant le tribunal ne précise pas pourquoi la loi trouve à s'appliquer, les motifs sont peu explicite. Google ayant fait appel de cette décision la solution reste à confirmer. Dans un deuxième jugement du TGI de Paris du 15 février 2012 le tribunal, dans une affaire similaire, a ordonné à Google.Inc de désindexer « les pages litigieuses ». Cependant le tribunal s'est surtout attaché à vérifier la responsabilité de Google au sens de la LCEN (devoir de désindexation quand un contenu illicite est signalé) et n'a pas évoqué la question de l'application territoriale de la LIL.

33 http://ec.europa.eu/civiljustice/glossary/glossary_fr.htm#LexLociDelicti

34 Le juge français est moins réticent à appliquer le droit commun et notamment lorsque l'atteinte est une atteinte à la vie privée TGI Paris, ordonnance de référé, 19 octobre 2006 Mme H.P. c/ Google France; et constitutive d'une infraction pénale, TGI Paris 17ème chambre, 6 novembre 2013, op.cit, « Attendu enfin, que la société défenderesse fait valoir que le tribunal ne pourrait réparer et ordonner des mesures d'interdiction visant d'autres sites que google.fr, qui ne visent pas le public de France [...];Attendu cependant [...] que le présent litige porte sur le référencement effectué grâce au moteur de recherche Google images que la société Google dit être seule à exploiter et à en avoir la maîtrise ; que, s'agissant d'images, il appartient à la société défenderesse de démontrer que les référencements sur des sites internet qu'elle exploite et qu'elle dit être destinés à un autre public que celui situé sur le territoire français, n'ont pas d'impact sur ce territoire où ces images ont été jugées constitutives d'une infraction pénale ;

Attendu, en conséquence, qu'il sera fait injonction [...]à la société Google Inc. de retirer et de cesser l'affichage sur le moteur de recherche Google images qu'elle exploite, accessible en France, des neuf images [...]; »

35 Considérant 21 de la directive n°95/46

que ce raisonnement est réservé au plan civil. En effet, l'article 113-2 du Code pénal dispose que : «La loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire » et la chambre criminelle, notamment en matière de contrefaçon, retient l'application de la loi pénale française, pour les infractions commises sur l'Internet, dès lors que le public français est visé[36]. Par analogie (faute de jurisprudence en la matière) il est alors aisé de considérer que la loi pénale française serait applicable à un responsable de traitement établi hors de l'Union européenne, pourvu que l'atteinte portée aux données à caractère personnel soit constitutive d'une infraction pénale[37]. Le bilan de la protection des données à caractère personnel garantie par le droit positif est mitigé, de par les limites sus-évoquées mais également par le manque d'effectivité que certains auteurs déplorent. Si ces limites sont incontestable, il convient de se pencher sur la notion de « droit à l'oubli numérique » qui semble émerger timidement et que la Loi Informatique et Libertés ne fait qu'évoquer. S'interroger sur la définition et sur la place du droit à l'oubli dans l'échelle des normes, c'est le positionner au regard du droit au respect de la vie privée (ce que l'on a brièvement envisagé dans les précédents développements[38]) mais également le sortir de la sphère de ce droit pour l'ériger en droit autonome. Le droit à l'oubli mérite ainsi d'être défini plus précisément car s'il en existe un embryon dans notre droit positif, la perpétuelle croissance que connait l'Internet, appelle des solutions plus pertinentes et adéquates.

Section 2- Le projet de règlement européen et la consécration du droit à l'oubli numérique.

11. Le projet de règlement européen. Le 25 janvier 2012, la Commission européenne a publié un projet de règlement « 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 » appelé à remplacer la directive 95/46/CE du 24 octobre 1995, jugée inadaptée aux développements des technologies et de la société. Ce projet a pour ambition de réformer en profondeur le régime existant en introduisant à la fois des mesures de simplification mais aussi, et pour l'essentiel de la réforme, des mesures de durcissement notamment en matière d'obligations à la charge des responsables de traitement. Ce projet donne l'occasion de son étude au regard du droit positif. Cette étude doit également inclure le rapport portant propositions d'amendements[39] rédigé par M. Albrecht[40], rapporteur de la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE ci après « Commission ») du Parlement européen, publié le 8 janvier 2013. La version

36 Cassation criminelle 14 décembre 2010, n° 10-80.088

37 Mais les infractions en la matière sont en constante augmentation

38 Sur ce point se référer à la contribution du Professeur Jean-Michel Bruguière « Le droit à l'oubli et les droits de la personnalité »

39 Plus de 3 000 amendements ont été déposés par les élus. Une majorité d'entre eux avait pour but d'amoindrir la protection (1 236, contre 943 en faveur de son accroissement ; 953 amendements sont considérés comme « neutres »). Mais seuls 350 amendements ont été intégrés au projet de la Commission publié en janvier 2013.

40 Jan Philipp Albrecht Groupe des Verts Allemagne/Alliance libre européenne

amendée du projet a été votée en Commission le 21 octobre 2013[41], le Parlement européen s'est donc doté d'un mandat pour négocier le texte avec le Conseil de l'Union européenne. Le rapport de la Commission a rapidement été déposé pour première lecture le 22 novembre 2013 et le Conseil de l'UE s'est déjà réuni une première fois le 6 décembre 2013. La séance plénière est prévue pour le 11 mars 2014 avant la fin de la législature du Parlement européen[42].

12. Apports du projet de règlement. Le choix d'un projet de règlement pour établir ce nouveau cadre n'est pas un hasard. Un règlement, d'applicabilité directe (article 288 TFUE[43]), permettra l'instauration d'un corps harmonisé de règles réduisant ainsi la fragmentation législative qui existe aujourd'hui entre les Etats membres. En effet, comme l'on a pu l'évoquer plus haut, la directive n°95/46 ne fait que fixer des objectifs à atteindre, laissant ainsi aux Etats membres une liberté sur certaines questions fondamentales comme la définition même de la notion de donnée à caractère personnel. Sur cette question, le projet de règlement vient uniformiser la notion puisqu'il retient qu'est une donnée personnelle « toute information se rapportant à une personne concernée[44] ». Cette définition a été élargie pour deux raisons principales :

- inclure les personnes qui peuvent être identifiées par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne (ce qui n'est pas nouveau en droit français[45] puisque la Loi Informatique et Libertés précise déjà que 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).
- inclure les personnes susceptibles d'être identifiées par référence à un identifiant en ligne ou à des données de localisation. Ainsi, le projet s'adapte aux nouvelles technologies en faisant de l'adresse IP et des identifiants cookie des données personnelles.

Outre cette extension du champ d'application « ratione personae » de la règlementation en matière de protection des données à caractère personnel au travers l'élargissement de cette

---

41 A l'heure où cette contribution est rédigée, il n'existe encore aucune version officielle de ce texte.

42 Cf la fiche de procédure : http://www.europarl.europa.eu/oeil/popups/printficheglobal.pdf?id=601375&l=fr

43 Article 288 du TFUE : « Pour exercer les compétences de l'Union, les institutions adoptent des règlements, des directives, des décisions, des recommandations et des avis.
Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre.
La directive lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. [...] »

44 Article 4 (1) et (2) du projet de règlement : «personne concernée»: une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; «données à caractère personnel»: toute information se rapportant à une personne concernée.

45 Mais qui l'est en droit anglais. Cf sur ce point la contribution du Professeur François Viangalli

notion, deux nouveautés doivent attirer notre attention. La première tend à une meilleure prise en compte du caractère international de l'Internet :

. La détermination de la loi applicable en cas d'atteinte.

En effet, la Loi Informatique et Libertés, au risque de me répéter, soumet à son application les traitements dont le responsable est établi sur le territoire français ou lorsque sans y être établi il recourt à des moyens de traitements qui y sont situés. Ainsi, l'on raisonne, selon Murielle Bénéjat, « d'un point de vue plus personnel – sur le responsable de traitement – que matériel – sur les données » instaurant une certaine insécurité juridique par la non application des droits nationaux à chaque fois que le responsable du traitement est établi hors de l'Union européenne.

Le projet de règlement et plus précisément les propositions de M. Albrecht suivant sur ce point l'avis du G29[46], préconise aujourd'hui de retenir le critère du « ciblage » des ressortissants de l'Union européenne pour justifier de l'applicabilité du règlement. Ce critère n'est pas nouveau puisqu'il existe déjà dans d'autres branches du droit et notamment en droit de la consommation autorisant ainsi un consommateur à s'adresser à l'autorité nationale dès lors qu'un service lui est fourni sur le territoire où il réside[47].

. Le dispositif du guichet unique.

Dans un souci de simplification, lorsque le responsable de traitement est établi dans plusieurs Etats membres, le projet de règlement prévoit d'accorder une compétence exclusive à l'autorité de contrôle du pays dans lequel est établi le « principal établissement[48] » du responsable.

12 bis. La seconde tend à la consécration d'un droit à l'oubli numérique autonome. L'article 17 du texte prévoit « un droit à l'oubli numérique et à l'effacement » c'est-à-dire le droit pour chaque « personne concernée » d'obtenir « du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données ». Si le droit positif déduit le droit à l'oubli numérique du droit à l'effacement (contenu lui-même dans le droit de rectification) ou du principe de proportionnalité énoncé à l'article 6 al.5 de la Loi Informatique et Libertés, le projet de règlement l'érige quant à lui en un droit autonome[49], instaurant dans le même temps son corollaire : un droit à l'effacement (qui sort ainsi de la sphère du droit de rectification) *Intérêt de l'autonomisation du droit à l'oubli numérique*. L'on évoquait jusqu'à

---

46 Le Groupe de travail Article 29 sur la protection des données ou G29 est un organe consultatif européen indépendant sur la protection des données et de la vie privée. Son organisation et ses missions sont définis par les articles 29 et 30 de la directive 95/46/CE, dont il tire sa dénomination, et par l'article 14 de la directive 97/66/CE.

47 Notion d'activité commerciale ou professionnelle dirigée vers l'État du domicile du consommateur. Article 15 et 16 du règlement n°44/2001du Conseil, du 22 décembre 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale.

48 Article 4 (13) du projet de règlement : «établissement principal»: en ce qui concerne le responsable du traitement, le lieu de son établissement dans l'Union où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement de données à caractère personnel; si aucune décision de ce type n'est prise dans l'Union, l'établissement principal est le lieu où sont exercées les principales activités de traitement dans le cadre des activités d'un établissement d'un responsable du traitement dans l'Union; en ce qui concerne le sous traitant, on entend par «établissement principal» le lieu de son administration centrale dans l'Union.

49 Se déduit de l'intitulé même de l'article 17 du projet de règlement : « droit à l'oubli numérique et à l'effacement »

système prôné par le règlement crée une distorsion entre le droit au recours juridictionnel que la personne concernée pourrait continuer d'exercer devant son juge national alors que le recours administratif contre ce même responsable de traitement relèverait de la seule compétence de l'autorité de contrôle étrangère établie dans le pays où le responsable du traitement aurait son établissement principal. Afin de remédier à cette distorsion, M. Albrecht préconise de rétablir la compétence respective des autorités tout en conférant à l'une d'entre elle (celle du pays dans lequel se trouve l'établissement principal du responsable de traitement) la qualité de chef de file. Si cette proposition a le mérite de coordonner les relations entre les différentes autorités de contrôle, elle ne résout cependant pas entièrement le problème d'asymétrie entre le recours juridictionnel et administratif ; l'autorité du lieu de résidence de la personne concernée ne devenant qu'une simple boite aux lettres. Certains auteurs constatent également que de nombreuses questions restent encore en suspens. Sur quel(s) fondement(s) admettre qu'une décision d'une autorité nationale ait une portée extraterritoriale ? Comment rendre les sanctions, adoptées selon cette procédure, applicables dans les autres Etats ? Concernant l'effectivité du droit à l'oubli numérique d'autre part. En effet, les modalités d'exercice du droit à l'oubli numérique par les personnes concernées ne saurait être efficace dès lors que les obligations des moteurs de recherche ne sont pas dans le même temps significativement renforcées. Le G29 suggère par exemple, qu'il soit prévu à la charge de ces prestataires une obligation positive de procéder à l'effacement automatique des contenus indexés dans un délai maximal à déterminer. La CNIL propose par exemple la mise en place d'un référentiel standard, une sorte de « date de péremption » assignée au contenu indexé. L'on peut légitimement s'interroger sur la pertinence de cette proposition tant il apparaît peu probable qu'une telle contrainte puisse être imposée aux moteurs de recherche[54].

Le G29 s'est alors réorienté, de façon plus réaliste, vers la possibilité pour tout intéressé de solliciter la désindexation des contenus qui lui portent préjudice (le critère du préjudice se substituerait ainsi au critère de l'absence d'intérêt légitime du responsable du traitement actuellement prévu par le règlement[55]). En ce sens, la CNIL appuyée par certains acteurs politique préconise également « un droit au déréférencement » qui permettrait d'exiger des moteurs de recherche « la suppression du référencement des informations » ayant fait l'objet d'une demande de droit à l'oubli. Pour la défenseure des enfants par exemple, une telle mesure serait un «corollaire indispensable d'une mise en œuvre du droit à l'oubli numérique» c'est-à-dire de son effectivité.

Conclusion

54 Solution également limitée par la duplication des informations indexées (copier/coller)

55 Critère que l'on retrouve à l'article 6-1.f) de la proposition de règlement : [...] « le traitement est nécessaire aux fins des intérêts légitimes poursuivis par un responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée, qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. Ces considérations ne s'appliquent pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions. » ou encore à l'article 19 : « La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à ce que des données à caractère personnel fassent l'objet d'un traitement fondé sur l'article 6 [...]à moins que le responsable du traitement n'établisse l'existence de raisons impérieuses et légitimes justifiant le traitement, qui priment les intérêts ou les libertés et droits fondamentaux de la personne concernée. »

présent le droit à l'oubli numérique que comme « le reflet du droit au respect de la vie privée » sur Internet, permettant de rendre effective la protection des données à caractère personnel. Toutefois il est vite apparut nécessaire de détacher ces notions, ces dernières ne recouvrant pas les mêmes éléments[50], afin de permettre une autonomisation du droit à l'oubli numérique. Le droit à la protection des données à caractère personnel, même si certains auteurs le contestent, connait déjà une autonomisation dans notre droit comme en témoigne par exemple l'article 8 de la Charte européenne des droits fondamentaux[51] qui consacre déjà, à côté du droit à la protection de la vie privée, une protection distincte des données à caractère personnel. Mais s'arrêter à ce stade serait garantir aux internautes la jouissance du droit à la protection des données à caractère personnel et non son effectivité, effectivité qui se trouve garantie par l'autonomisation du droit à l'oubli numérique. Pendant un temps, des auteurs s'interrogèrent sur la justesse de l'appellation « droit » à l'oubli. Il y aurait selon l'un d'entre eux un abus du mot droit dans la mesure où l'oubli n'emporte qu'une obligation à la charge d'autrui, sans qu'aucune prérogative ne soit conférée à l'intéressé[52]. Que doivent alors penser ces auteurs de la demande du G29 quant à la consécration d'un tel droit au rang de droit fondamental particulier[53] ? Outre ces avancées, le projet de règlement évince également les fragilités tenant à la rédaction actuelle de la Loi informatique et Libertés évoquées plus haut et par exemple « le motif légitime » qui conditionne l'exercice par la personne concernée du droit d'opposition devient « sa situation particulière », l'effectivité du droit d'accès est garantie par l'instauration de son corollaire à savoir le droit à la portabilité des données.

13. Limites du projet de règlement et solutions prospectives. De manière générale le projet de règlement renforce les obligations incombant au responsable de traitement (l'obligation d'information notamment) laissant une place phare au consentement de la personne concernée, ainsi, l'on peut craindre que celles-ci ne viennent encore accentuer le décalage entre les législations européennes et américaines. Les avancées sus mentionnées sont loin de faire l'unanimité, partant, de nombreuses réserves peuvent être mises en lumière. Concernant la prise en compte du caractère transfrontière de l'Internet d'une part. L'élargissement de la portée du droit européen instauré par le projet de règlement avec le critère de « ciblage » des ressortissants européens ne sera pertinent qu'à la condition que les décisions prises ou sanctions prononcées soient susceptible d'exécution pratique. Un certain pessimisme est ici autorisé. Dans le même sens, l'instauration du système du guichet unique appelle quant à elle une vive opposition du G29 compte tenu du déséquilibre qu'entrainerait une telle mesure s'agissant du traitement réservé aux plaintes des personnes concernées. Il convient en effet de rappeler ce que l'on a énoncé précédemment, le guichet unique attribuerait une compétence exclusive à l'autorité nationale de contrôle du pays dans lequel le responsable de traitement a son établissement principal aux fins d'instruire et de juger les plaintes administratives des personnes concernées. Le G29 relève que le

---

50 Cf, développement dans l'introduction

51 Article. 8.1 Protection des données à caractère personnel : « Toute personne a droit à la protection des données à caractère personnel la concernant ».

52 P. Kayser, la protection de la vie privée par le droit, 2e éd. In: Revue internationale de droit comparé. Vol. 43 N°1, Janvier-mars 1991. pp. 269-271.

53 CNIL, 21ème Rapport d'activité 2000, p. 187

Si le projet de règlement contient de nombreuses avancées et notamment l'harmonisation du droit des Etats membres de par l'essence même du règlement, certaines questions relatives aux contours du droit à l'oubli numérique subsistent.

Le droit à l'oubli numérique serait donc un droit autonome qui permettrait à toute personne de demander au site publiant des données à caractère personnel la concernant d'en obtenir le retrait après l'écoulement d'un certain laps de temps ; un retrait effectif puisque la personne concernée pourra exiger du responsable de traitement que la donnée la concernant soit déréférencée (dans le cas ou le projet de règlement retienne la proposition du G29) ; un déréférencement ou *à minima* un effacement conditionné à l'atteinte portée au dit droit à l'oubli ; atteinte caractérisée soit par la conservation de la donnée au delà de la finalité prescrite, soit par la conservation de la donnée après le retrait du consentement de la personne concernée ou lorsque la personne concernée s'oppose au traitement. Ces conditions d'exercice du droit à l'oubli ne sont pas nouvelles puisqu'elles existent déjà dans notre droit, autrement dit l'article 17 rassemble en fait des situations qui correspondent davantage à des traitements illicites ou devant de toute façon cesser : l'hypothèse de l'inadéquation des données traitées à la finalité déclarée du traitement par exemple. Il s'agit là, en effet, de la répétition de droits déjà accordés, ceux d'opposition et de retrait et le droit de demander l'effacement en cas de traitement illicite. La seule nouveauté résiderait-elle dans la consécration textuelle du droit à l'oubli numérique[56] ? L'on peut également soulever la question de l'effectivité de cette protection qui reste à certains égards remise en cause et qui révèle la difficile intervention juridique sur un « terrain mondial ». En effet, si le droit « à l'oubli numérique et à l'effacement » est le pendant nécessaire à l'effectivité de la protection des données à caractère personnel, c'est à la condition que soient instaurées des prérogatives garantissant l'effectivité du dit droit à l'oubli. Peut être devrait on responsabiliser l'internaute plutôt que de le « surprotéger » avec une protection en demie teinte. Une *question restée à l'écart des débats attire, pour finir dans un élan d'optimisme, notre attention, à savoir, la propriété sur les données à caractère* personnel. Certains auteurs considérant même qu'il existe en la matière « un vide juridique, qu'il faut impérativement combler ». De nombreuses plates-formes revendiquent la propriété pure et simple des données à caractère personnel postées par les internautes[57]. Dans ce domaine, les auteurs s'accordent sur l'indispensable « intervention du législateur pour créer un droit de propriété qui soit personnel, incessible et inaliénable ». Il s'agit d'un enjeu majeur qui pourrait alors redéfinir les règles du jeu.

---

56 Consécration qui n'existe pas dans la version anglaise du texte qui n'évoque que le « right to erasure »

57 Article 2.2 CGU LinkedIn : « ...De plus, vous concédez à LinkedIn un droit non exclusif, irrévocable, pour le monde entier, perpétuel, illimité, cessible, qui peut être l'objet de sous-licences, entièrement payé et libre de toute obligation à payer une redevance, de copier, élaborer des œuvres dérivées, améliorer, diffuser, publier, retirer, retenir, ajouter, analyser et utiliser ou commercialiser de toute façon actuellement connue ou à venir, tout élément que vous fournissez, directement ou indirectement, à LinkedIn, et notamment tout contenu généré par un utilisateur, toute idée, tout concept, toutes techniques ou données que vous soumettez à LinkedIn, sans autre autorisation, notification, et/ou contrepartie pour vous ou tout autre tiers. Toute contribution que vous nous soumettez l'est à vos risques.... »

Retour à la case départ !

CHAPITRE 2

Le droit à l'oubli appliqué aux personnes morales[1]

1. La personnalité morale. La personnalité juridique est traditionnellement définie comme : « l'aptitude à être titulaire de droits et assujetti à des obligations qui appartient à toutes les personnes physiques, et dans des conditions différentes, aux personnes morales »[2]. L'intérêt de cette définition de la personnalité juridique est double. Dans un premier temps, la personne morale est apte à être titulaire de tous droits pécuniaires et extrapécuniaires sous réserve du principe de spécialité légale et statutaire, même si pour pouvoir exercer ses droits, la personne morale doit recourir à des personnes physiques[3]. Dans un second temps, la définition enseigne sur la construction même des droits des personnes morales. En effet, par les termes « dans des conditions différentes », on peut considérer que les droits accordés aux personnes physiques ne seront pas strictement les mêmes que ceux des personnes morales. Plus positivement, le contenu de leurs droits s'adapte à leurs spécificités, à leurs besoins et à leurs objectifs, qui sont exprimés notamment pour les entreprises sociétaires par la collectivité des associés dans les statuts. Grâce à sa personnalité juridique, la personne morale peut prétendre au bénéfice d'un droit à l'oubli de ses informations, si ce droit lui donne les moyens de la réalisation de ses objectifs.
Il est question des personnes morales constituées sous forme de société, et ayant acquis la personnalité morale par le simple fait de leur immatriculation. La réflexion peut être aisément transposée à toutes les personnes morales de droit privé, telles que notamment les groupements, syndicats et associations. L'exception doit être ici faite des personnes morales de droit public dont la sensibilité des informations traitées nécessite un examen particulier. L'exception porte également sur les entreprises individuelles (artisan, commerçant ou profession libérale), pour lesquelles l'atteinte aux informations personnelles se confond nécessairement avec celles portées à la personne physique.

2. Les informations à protéger des personnes morales : les enjeux. L'entreprise expose et s'expose sur Internet. La maîtrise des informations concernant son image, ses produits ou services représente un enjeu commercial stratégique. D'une part, l'entreprise double son identité réelle d'une identité virtuelle, en opérant un contrôle de l'ensemble des informations qui lui sont relatives sur Internet et plus précisément sur les moteurs de recherche et les réseaux sociaux. D'autre part, l'entreprise peut agir à augmenter le trafic et la visibilité de son site web et des espaces sociaux qu'elle occupe. Elle crée ainsi du lien avec les internautes afin de pérenniser la relation client. En effet, 85% des consommateurs cherchent une information sur un produit

---

1 Par Amélie Favreau, Maître de conférences à l'Université Grenoble Alpes.

2 G. CORNU, Vocabulaire juridique, Association H. Capitant, V° Personnalité, PUF.

3 En ce sens, voir notamment les articles 223-22, 225-21, 225-25, 225-53 du Code de commerce.

avant de le consommer et 73% seraient influencés par les avis des autres consommateurs[4]. Enfin, l'entreprise participe à l'intelligence économique[5], c'est-à-dire qu'elle conduit des stratégies industrielles qui reposent sur sa capacité à accéder aux informations. Ces différents enjeux se recoupent dans la maîtrise par l'entreprise de ce qu'il convient d'appeler sa réputation, et plus précisément sur Internet son « e-réputation ». Nous avons eu l'occasion de la définir comme : « l'action d'une personne physique ou morale pour maîtriser l'évaluation sociale portée sur son image numérique »[6]. Les deux points forts de cette définition sont : d'un côté l'affirmation que les informations d'une entreprise divulguées sur la toile sont soumises à l'évaluation sociale. En effet, elles font nécessairement appel à un jugement, qui impliquera un classement basique entre une « bonne » ou « mauvaise » réputation ; et d'un autre côté, l'idée soutenue que la réputation d'une entreprise se gère. C'est un point sur lequel juristes, économistes et stratèges en marketing se retrouvent. Dans notre actuelle société de connaissance, l'exposition indispensable pour une entreprise peut également être destructrice, comme en témoignent les récentes affaires Findus, Ikéa ou Nestlé qui ont fait « le buzz », plus précisément le « bad buzz », pour des raisons sanitaires ou écologiques. Une réputation et ce d'autant plus sur Internet se construit, bien gérée elle ne doit pas être subie par l'entreprise. Ainsi les manipulations de la technique se mettent au service d'un modelage de la perception globale d'une marque, d'une entreprise ou d'un produit et génèrent le « good buzz ». Le contrôle porte autant sur l'information divulguée par l'entreprise et que sur l'information de l'entreprise diffusée par les tiers, les consommateurs, les salariés. Pour assurer ces contrôles, les agences d'e-réputation fleurissent. Le droit à l'oubli peut donc apparaitre comme un moyen mis à disposition des entreprises pour procéder à la gestion de l'évaluation sociale, autrement dit à la maîtrise de leur « e-réputation ».

3. Du droit à l'oubli au droit à l'effacement. L'engouement doctrinal[7] et médiatique[8] pour le « droit à l'oubli » motive la réalisation de cette étude. Il sonne comme un slogan aux revendications aisées, alors qu'il est aujourd'hui complexe d'en dessiner ses contours et de lui assigner un fondement. Le droit à l'oubli, malgré une tentative avortée française[9], ne fait pas

---

4 M. QUEMENER et G. HAAS, E-réputation, regards croisés de l'avocat et du magistrat sur l'e-réputation négative, Expertises n°332, octobre 2011, p. 337.

5 Rapport d'Henri Marte, Rapport du Groupe « Intelligence économique et stratégie des entreprises », La documentation française, 1994.

6 A. FAVREAU, Protéger l'e-réputation de l'entreprise, Colloque du CUERPI, 6 décembre 2013, L'entreprise à l'épreuve du droit de l'Internet, Quid novi ?, actes à paraître.

7 Une des premières contributions sur le sujet est celle de C. COSTAZ, Le droit à l'oubli, Gaz. Pal, 27 juillet 1995, II, doctr. P. 961. V. aussi Commission des lois du Sénat, Rapport d'information n°441 (2008-2009), La vie privée à l'heure des mémoires numériques, de M. Y. DETRAIGNE et Mme A.-M. ESCOFFIER, p. 35 ; N. MALLET POUJOL, Du droit à l'oubli numérique, Litec, RD&J, n°37, nov. 2011, p. 9.

8 Parmi la quantité d'articles de journaux consacrée au droit à l'oubli, nous prendrons simplement l'exemple de la réaction du quotidien Le Monde, le 8 octobre 2011, à la délibération de la CNIL sur l'association LEXEEK (CNIL, délib. n° 2011-238 de la formation restreinte, 12 juill. 2011 : www.cnil.fr), ou encore Droit à l'oubli : "Actuellement, il manque des solutions juridiques", par Yann Padova, secrétaire général de la Commission de l'informatique et des libertés, le Monde, 08.10.11.

9 En ce sens, la proposition de loi n°93 visant à mieux garantir la vie privée à l'heure du numérique, déposée au Sénat le 6 novembre 2009 par M. Y. DETRAIGNE et Mme A.-M. ESCOFFIER, qui apporte des recommandations censées aux nouveaux défis du numérique.

encore l'objet d'une consécration législative générale. Moins encore la Commission LIBE du Parlement européen lors du vote du 21 octobre 2013 l'a finalement supprimé du texte de la Commission européenne du 25 janvier 2012[10]. En effet, la Commission européenne qui a déposé une proposition de Règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données)[11], prévoyait en son article 17, intitulé Droit à l'oubli numérique et à l'effacement, la possibilité pour « la personne concernée » d'obtenir « du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était enfant » ou pour d'autres motifs énumérés dans l'article. L'amendement n°118 adopté par la Commission LIBE remplace l'expression consacrant le droit à l'oubli et à l'effacement (« Right to be forgotten and to erasure ») par le simple droit à l'effacement (« right to erasure ») tant dans l'intitulé de l'article 17 que dans l'ensemble du texte. La Commission LIBE justifie que les termes seraient « misleading », à savoir « trompeur », « déceptif ». La consécration ambitieuse d'un droit à l'oubli au niveau européen n'aura pas lieu. En effet, le Parlement européen, confirmant cette dernière version, a adopté par une large majorité, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données)[12]. Nous conserverons toutefois dans la suite de cette contribution l'expression « droit à l'oubli », considérant qu'elle peut avoir une résonnance plus large dans le droit positif national.

4. Droit à l'oubli pour les personnes morales et droit à l'oubli pour les dirigeants sociaux. La personnalité d'une personne morale doit être distinguée de celle de ses membres, y compris de celle de ses dirigeants, et ce quand bien même la structure serait unipersonnelle. En d'autres termes, étudier la titularité du droit à l'oubli pour les dirigeants de sociétés, associés ou actionnaires de groupement personnifié, personnes physiques n'a aucune incidence sur l'admission des personnes morales au bénéfice de la protection de leurs informations par les dispositions nationales, européennes ou internationales. La Commission nationale de l'informatique et des libertés (CNIL) a eu l'occasion de le rappeler à propos de fichiers d'entreprises. Ainsi sur le fondement de la loi du 6 janvier 1978, loi dite « Informatique et

10 Voir le Rapport 22 novembre 2013, Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) par Jan Philipp Albrecht sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

11 Commission européenne, Proposition de Règlement européen et du Conseil, 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, 25 janvier 2012, COM/2012, 11 final.

12 Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Voir notamment, amendement 112, relatif à l'article 17 de la proposition de Règlement.

Libertés »[13], elle considère que « si le droit d'accès établi par l'article 34 de la loi du 6 janvier 1978 a un caractère strictement individuel, il convient d'en reconnaître l'exercice aux personnes physiques, représentants légaux des entreprises, dès lors que le nom de ces personnes figure dans le fichier en tant que dirigeant, actionnaire ou associé »[14]. Dans le même sens, les dispositions du décret n°2013-799 du 2 septembre 2013 permettent la suppression du code 040 de la base de données du fichier bancaire des entreprises (FIBEN) de la Banque de France, affublant les dirigeants ayant conduit une société à la liquidation judiciaire[15]. L'oubli dont peuvent bénéficier des dirigeants ne peut être ici confondu avec l'effacement des données dont se prévalent déjà les personnes morales au titre des dispositions sur le redressement judiciaire[16].

5. L'intérêt du droit à l'oubli pour les personnes morales. L'intérêt du droit à l'oubli doit être ici considéré comme un outil permettant à la personne morale de réaliser une maîtrise des informations la concernant afin de susciter une évaluation sociale positive. Autrement dit, le droit à l'oubli est un moyen juridique au service de la construction de son « e-réputation ». La question est donc entière : ce droit à l'oubli est-il ouvert par le droit positif (et le proche droit prospectif) aux personnes morales ? Et si toutefois tel n'était pas le cas, les moyens juridiques actuellement mis à disposition des personnes morales pour organiser l'oubli et l'effacement de leurs informations ne conduiraient-ils pas aux mêmes effets ?
Il est dans un premier temps nécessaire de vérifier la titularité des personnes morales d'un droit à l'oubli se pose (1) avant de s'interroger sur l'intérêt de ce nouvel outil juridique (2).

Section 1- La difficile reconnaissance d'un droit à l'oubli pour les personnes morales

6. Présentation des difficultés. La question de la titularité du droit à l'oubli par des personnes morales se heurte à un double obstacle. Un regard sur la nature du droit à l'oubli – bien que cette question dépasse le cadre de cette étude – nous permet de comprendre les réticences de la doctrine à cette reconnaissance (I). Ces réticences doctrinales bien qu'elles puissent être surmontées sont confortées par les sources du droit à l'oubli. En effet, les personnes morales ne sont pas admises au bénéfice d'un droit à l'oubli par les textes actuels et à venir sur la protection des données à caractère personnel (II).

---

13 Loi n°78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, plus connue sous le nom de loi informatique et libertés de 1978. Elle a fait l'objet de nombreuses modifications. Les plus récentes sont celles de l'ordonnance n° 2011-1012 du 24 août 2011 (Journal officiel du 26 août 2011) et Loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique (Journal Officiel du 12 octobre 2013).

14 CNIL, Délibération n°84-28 du 3 juillet 1984, relative à la mise en œuvre par les mairies d'Arcueil, Gentilly, Ivry-sur-Seine, Villejuif et Vitry-sur-Seine, d'un fichier d'entreprises. V. aussi, J. FRAYSSINET, A propos du droit d'accès des personnes morales, Expertises, oct. 1984, n°66, p. 241.

15 H. BOURBOULOUX, Le décret du 2 septembre 2013 : le droit à l'oubli tout relatif des dirigeants ayant connu une procédure collective, JCP E, n° 46, 14 novembre 2013, act. 821.

16 En ce sens, l'article R. 626-20 al. 2 du Code de commerce qui dispose : « Si le plan est toujours en cours à l'expiration d'un délai de deux ans à compter de son arrêté, les mentions relatives à la procédure et à l'exécution du plan sont, à l'initiative du débiteur, radié des registres ou répertoires sur lesquels elles ont été portées. Cette radiation fait obstacle à toute nouvelle mention relative à l'exécution du plan ».

I- L'accueil relatif de la doctrine

7. La nature du droit à l'oubli. La question préalable à se poser est celle de la nature du droit à l'oubli. En effet, la titularité du droit et le régime juridique de ce droit dépendront de cette qualification. Que ce droit à l'oubli puisse être qualifié de droit de propriété ou considéré comme un élément de la personnalité, cette question demeure discutée et dépasse le cadre de notre étude. Nous retiendrons donc, avec l'insouciance liée aux obstacles de ces deux qualifications, le postulat suivant : le droit à l'oubli s'inscrit parmi les droits de la personnalité. Même si cette qualification est très discutable, la thèse « personnaliste » offre plus de débat et d'interrogations sur la titularité des personnes morales que si nous avions cédé à une logique « propriétariste ».

8. Les obstacles surmontés à la titularité des droits de la personnalité des personnes morales. Le débat s'inscrit dans un contexte d'anthropomorphisme[17] qui a divisé la doctrine sur la possibilité de reconnaître des droits de la personnalité aux personnes morales. La tendance doctrinale actuelle dépasse l'anthropomorphisme critiquable en proposant une construction de droits propres de la personnalité des personnes morales[18]. Trois types d'obstacles sont avancés pour nier l'existence de droits de la personnalité aux personnes morales[19]. Tout d'abord, le plus ancien daté de la célèbre formule de Gaston Jèze selon laquelle « il n'a jamais déjeuné avec une personne morale » consiste à déterminer si la personnalité morale relève d'une réalité, qui est à la fois psychosociologique, psychologique et institutionnelle ou d'une fiction, créée par la seule intervention législative. Le législateur ne peut pas attribuer par l'effet de la loi une existence psychosociologique ou psychologique. Ainsi, les attributs de la personne morale dans la théorie de la fiction seraient exclusivement patrimoniaux. Exit donc la possibilité pour une personne morale d'agir contre les atteintes portées à son honneur ou à sa réputation – et par extension à l'oubli de ses informations personnelles. La théorie de la fiction est particulièrement présente dans les textes 1842 du Code civil issu de la loi du 4 janvier 1978 et l'article 210-6 Code de commerce selon lesquels « les sociétés... jouissent de la personnalité morale à compter de leur immatriculation », c'est-à-dire attribuée artificiellement – fictivement - par l'ordre de la loi. Il convient à l'inverse de signaler un vieil arrêt de la 2ème chambre civile de la Cour de cassation qui consacre que l'essence de la personnalité morale réside dans sa volonté, dans sa conscience et dans ses œuvres[20].

---

17 En ce sens v. notamment, G. LOISEAU, Des droits humains pour des personnes non humaines, D. 2011, p. 2558 ; V. WESTER-OUISSE, Dérives anthropomorphiques de la personnalité morale : ascendances et influences, JCP G 2009. I. 137 et La jurisprudence et les personnes morales. Du propre de l'homme aux droits de l'homme, JCP G 2009, I, 121.

18 F. PETIT, Les droits de la personnalité confrontés aux particularismes des personnes morales, D. Aff. 1998, N°117, p. 826 ; L. DUMOULIN, Les droits de la personnalité des personnes morales, Revue des sociétés, 2006, p. 1 ; H. MARTRON, Les droits de la personnalité des personnes morales de droit privé, LGDJ 2011.

19 Ils ont parfaitement été synthétisés et discutés par J.-M. BRUGUIERE et B. GLEIZE, Les droits de la personnalité, à paraître.

20 Civ. 2ème 28 janvier 1954 : « la personnalité morale n'était pas une création de la loi, mais qu'elle appartenait en principe à tout groupement pourvu d'une possibilité d'expression collective pour la défense d'intérêts licites, dignes d'être juridiquement reconnus et protégés et qui sont distincts des intérêts individuels des membres du groupement » (in H. CAPITANT, F. TERRE, Y. LEQUETTE, Les grands arrêts de la jurisprudence civile, Dalloz, 12e éd., Tome

Un autre argument consiste à trouver la source des droits de la personnalité dans le concept de dignité. La dignité étant le propre de l'être humain, il est dès lors impossible d'étendre les droits qui en découlent aux personnes morales[21]. Comme il a été remarqué dans les propos introductifs, les droits des personnes morales n'ont pas nécessairement à être construits sur le décalque de ceux des personnes physiques. En ce sens, une décision récente de la Cour européenne des droits de l'homme, sur laquelle nous reviendrons dans la suite de cette étude, consacre la protection de la réputation d'une personne morale et la Cour a pris le soin de dissocier cette protection du concept de dignité[22].

Enfin, le dernier obstacle consiste en l'impossibilité d'admettre les personnes morales à l'indemnisation de leur préjudice moral à travers l'atteinte à un droit extrapatrimonial. Cette reconnaissance implique que les droits dont sont titulaires les personnes morales ne sont pas seulement patrimoniaux, mais comprennent des éléments comme l'image, l'honneur ou la réputation. L'indemnisation du préjudice moral des personnes morales devient selon les mots de Carbonnier un « fantasme de fantômes »[23]. Cet obstacle est dépassé depuis longtemps par la Cour de cassation[24]. Elle l'a réaffirmé dans un arrêt récent à propos d'actes de concurrence déloyale causant un préjudice financier et moral à une société commerciale[25]. Défini plus largement par une partie de la doctrine, le préjudice moral recouvre *« toute forme d'atteinte à la personnalité de la victime »*[26] et trouve dès lors à s'appliquer aux personnes morales.

Même si les obstacles doctrinaux peuvent être surmontés quant à l'admission des personnes morales à la protection de leurs droits de la personnalité, la solution législative exclut expressément les personnes morales des bénéfices de la protection des données personnelles.

II- L'écueil des sources du droit à l'oubli

9. La personne morale : bénéficiaire ou débitrice d'un droit à l'oubli ? En matière de données personnelles, il est possible de scinder les sujets d'un droit à l'oubli en deux principaux groupes. Il existe d'un côté les bénéficiaires d'un droit à l'oubli (A), qui exerceront le droit et solliciteront activement la protection de leurs données personnelles et d'un autre côté, se tenant à disposition des premiers, se trouvent les débiteurs (B).

---

1). Affirmation de la personnalité morale des comités d'établissement, dont la loi du 28 octobre 1982 devait reprendre la solution.

21 En ce sens, G. LOISEAU, Des droits patrimoniaux de la personnalité en droit français, Rev. Dr. Mc Gill, juin 1997, n°142 « c'est l'être humain comme tel qui par opposition à la chose, a une dignité motivant le respect. La considération de l'humanité en chacun détermine donc l'attribution des droits de la personnalité en la circonscrivant aux seules personnes humaines ».

22 CEDH, 19 juill. 2011, n° 23954/10, Uj c/ Hongrie, v. infra n°29.

23 J. CARBONNIER, Droit civil Les biens, Les obligations, PUF, 2004, n°1122.

24 En ce sens v. notamment : Crim. 7 novembre 1936, Gaz. Pal. 1936, 2, 944. Voir aussi la reconnaissance au niveau européen : CEDH 6 avril 2000, n°35382/97, Sté Comingersoll, à propos du préjudice moral résultant pour une société commerciale de l'atteinte à son droit à un procès dans un délai raisonnable.

25 Com., 15 mai 2012, D. 2012. 2285, obs. X. Delpech, note B. Dondero ; D. 2012. 2688, obs. J.-C. Hallouin, E. Lamazerolles et A. Rabreau ; Revue des sociétés 2012. 620, note P. Stoffel-Munck, RTD civ. 2013. 85, obs. J. Hauser ; JCP E 2012. 1510, note R. Mortier.

26 P. MALAURIE, L. AYNES et P. STOFFEL-MUNK, Les obligations, 5e éd., 2011, n°248.

A- L'exclusion des personnes morales au titre des bénéficiaires d'un droit à l'oubli

10. Une exclusion nationale, européenne et internationale. Qu'il s'agisse de la Loi Informatique et Libertés (a), de la proposition de règlement européen « Data protection » (b), ou encore de textes émanant du Conseil de l'Europe (c), les personnes morales sont formellement exclues du bénéfice de protection de leurs données personnelles.

a) Le refus actuel de la protection des personnes morales par la Loi Informatique et Libertés

11. La protection conférée par la Loi Informatique et Libertés. La loi du 6 janvier 1978, loi dite « Informatique et Libertés » dote pour la première fois la France d'un ensemble de règles en vue d'une défense de l'individu face aux risques de l'informatique. Cet objectif est énoncé dès l'article 1er de la loi qui dispose que : « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».
Même si à l'époque la loi consistait à protéger les individus contre le traitement des fichiers informatiques par l'administration, elle contient les premiers outils juridiques vers une possible consécration générale d'un « droit à l'oubli », et plus précisément de ce qu'une partie de la doctrine appelle le « droit au retour à l'anonymat »[27]. On peut lire en ce sens les dispositions de l'article 6 5° de la loi Informatique et Libertés, selon lequel les données « sont conservées 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 ».
L'inviolabilité des données personnelles est également garantie sur le fondement de l'article 38 de la loi qui permet à toute personne physique de s'opposer, pour des motifs légitimes, à ce que ses données personnelles fassent l'objet d'un traitement. Cette prérogative est complétée par des droits d'accès et de rectification qui autorisent toutes personnes physiques à agir pour le maintien de la véracité des informations les concernant.

12. L'exclusion des personnes morales de la protection. La loi Informatique et Libertés exclut expressément les personnes morales de la protection qu'elle instaure. L'article 2, al. 2 de la loi définit la donnée à caractère personnel comme « 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 ». Et l'article 1er, nous le rappelons, protège le « citoyen » dans son « identité humaine ».
Cette loi ne permet pas aux personnes morales de se prémunir contre les risques inhérents à la violation de leurs informations. D'une part, la personne morale n'a pas la faculté sur le fondement de la Loi Informatique et Libertés de s'opposer au traitement fait par une autre personne physique ou morale des informations la concernant. La loi n'impose pas aux personnes physiques ou morales qui sont susceptibles d'utiliser une information concernant la société, l'association ou le syndicat d'en recueillir le préalable consentement. D'autre part, la collecte des informations détenues sur une personne morale est libre, c'est-à-dire qu'elle n'est pas soumise à

27 J.-C. SAINT-PAU (sous la dir.), Droits de la personnalité, Lexisnexis, coll. Traités, 2013, n°969, p. 596.

des finalités de traitements identifiées au moyen d'une déclaration. La personne morale ne peut donc pas se prévaloir de l'effacement de ces informations une fois la finalité du traitement réalisée. Enfin, la personne morale ne dispose pas par l'effet de cette loi des bénéfices de rectification ou d'accès aux informations traitées par autrui.

En conclusion, l'ensemble de la protection organisée par la loi Informatique et Libertés des informations relatives à l'identité des personnes physiques ne s'applique pas aux personnes morales. En d'autres termes, les atteintes portées aux informations relatives à une personne morale et ayant fait l'objet d'un traitement informatique ne sont pas être sanctionnées sur le fondement des dispositions de la Loi Informatique et Libertés.

b) Le prochain refus de la protection des personnes morales par la proposition de Règlement européen

13. La protection conférée par la proposition de Règlement européen. Succinctement, il convient de rappeler que le la proposition de Règlement européen 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 émanant de la Commission européenne, récemment amendée par le Parlement européen, prévoit un nouveau cadre juridique pour la protection des données à caractère personnel dans l'Union européenne. Les principes relatifs au traitement des données à caractère personnel correspondent à ceux de la directive 95/46/CE[28]. La proposition de Règlement apporte des précisions sur des droits connus comme le droit à l'information et à l'accès aux données, à la rectification et à l'opposition ou au profilage. Elle introduit également des éléments nouveaux, comme le principe de transparence ou le droit à l'oubli numérique et à l'effacement, qui subsistent seulement en l'expression d'un « droit à l'effacement ».

14. L'exclusion des personnes morales de la proposition de Règlement européen par la Commission européenne. Le titre même de la proposition de Règlement laisse peu d'espoir sur l'inclusion des personnes morales au titre des bénéficiaires d'un droit à l'oubli, puisqu'il est 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 ».
Cette exclusion est par la suite confirmée par toute une série de dispositions insérées dans la proposition de Règlement. Tout d'abord, dès le préambule, il est précisé que la protection conférée par le présent règlement concerne « les personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, dans le cadre du traitement des données à caractère personnel ». De plus, l'article 4 du projet de règlement définit la « personne concernée », visée à l'article 17 de la proposition de règlement, comme : « une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement (...) ». Ensuite, cette proposition est confirmée dès l'article 1er du projet : « Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données ». Enfin, l'article 89 de la

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, JO L 281 du 23.11.1995, p. 31.

proposition de règlement, à des fins d'uniformisation[29], prévoit *in fine* la suppression de l'article 1er, paragraphe 2, de la directive 2002/58/CE[30]. Cette directive admettait les personnes morales à la protection des intérêts légitimes des abonnés dans le secteur des communications électroniques.

En conclusion, il est par ces différents éléments fermement exclu que les personnes morales puissent prétendre au cadre juridique envisagé pour la protection des données à caractère personnel dans l'Union européenne par la proposition de Règlement européen, quand bien même elles démontreraient que leur nom, leur forme juridique et leurs coordonnées seraient des données nécessitant une protection équivalente à celle des personnes physiques.

15. L'exclusion confirmée par le Parlement européen. Cette exclusion est confortée par la Commission Libertés civiles, justice et affaires intérieures (LIBE)[31] et a été confirmée par l'adoption le 12 mars 2014 par le Parlement européen en formation plénière de la proposition de Règlement européen relative à protection des données personnelles[32].

Notamment, à l'article 4 de la proposition de règlement européen sur la protection des données personnelles, le Parlement supprime la définition relative aux « personnes concernées », mais souligne que les "*'personal data' means any information relating to an identified or identifiable natural person ('*data subject'); *an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person".*

Les articles 1er et 89 précités ne sont pas amendés par la Commission LIBE, concernant les personnes morales et sont adoptés par le Parlement européen le 12 mars 2014. En conclusion, la version la plus récente de la proposition de Règlement européen sur la protection des données personnelles ne prévoit pas l'extension de son objet et de son champ d'application aux personnes morales.

---

29 Ainsi, la référence à l'article 114, paragraphe 1, du TFUE n'est nécessaire qu'aux fins de modification de la directive 2002/58/CE.

30 Article 1er de 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 (directive vie privée et communications électroniques), qui dispose : « 1. La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté. 2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales ». La partie soulignée étant celle supprimée par le projet de règlement européen.

31 Rapport 22 novembre 2013, Commission des libertés civiles, de la justice et des affaires intérieures par Jan Philipp Albrecht sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

32 Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

c) Le prochain refus de la protection des personnes morales par le Conseil de l'Europe

16. L'histoire commença par une admission des personnes morales... La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été élaborée au sein du Conseil de l'Europe et adoptée le 28 janvier 1981[33]. Elle a pour objet de renforcer la protection des données, c'est-à-dire la protection juridique des individus vis-à-vis du traitement automatisé des données à caractère personnel les concernant.
En son article 3 sur le Champ d'application, elle consacre que tout État « appliquera la présente Convention également à des informations afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique ».

17. ...et l'histoire se terminera par une exclusion des personnes morales. La Convention fait actuellement l'objet d'une modernisation. Ainsi, le document final daté du 16 octobre 2012[34] raye les précédentes dispositions ouvertes au bénéfice des personnes morales. Le champ d'application de la Convention ne précise plus les titulaires de la protection. Il est pour cela nécessaire de se reporter à l'article 2, qui indique que les données personnelles sont les informations concernant une personne physique[35]. Le seul avantage de l'exclusion prochaine des personnes morales de la protection internationale sur les données personnelles est de créer une uniformité des textes nationaux, européens et internationaux.

B- La réception des personnes morales au titre des débiteurs d'un droit à l'oubli

18. Une reconnaissance unanime. L'ensemble des textes nationaux, européens et internationaux admet la personne morale comme débitrice d'une obligation de protection des données personnelles. Il ne nous semble pas nécessaire de réaliser l'inventaire des obligations incombant aux personnes morales en reprenant chacun des textes précédemment évoqués. Nous nous attacherons donc à identifier cette obligation au regard du droit à l'oubli consacré par la proposition de Règlement européen, plus précisément à travers l'acte d'effacement (a) et à évoquer l'obligation générale d'accountability qui concerne les personnes morales (b).

a) La personne morale débitrice d'une obligation d'effacement

---

33 Conseil de l'Europe, Convention STE n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ratifié par la France le 24 mars 1983 et entré en vigueur le 1er octobre 1985.

34 Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n°108, Strasbourg le 16 octobre 2012, Propositions de modernisation adoptées par la 29e réunion plénière, T-PD(2012)4Rev4, article 3, al. 2b : Biffer.

35 Article 2 de la proposition de modernisation de la Convention STE n°108 : « données à caractère personnel» signifie : toute information concernant une personne physique identifiée ou identifiable («personne concernée») »

19. La réception des personnes morales au titre des débiteurs par la Commission européenne. Si les personnes morales ne sont pas considérées comme bénéficiaires d'un droit à l'oubli, elles sont clairement identifiées comme les débitrices de ce droit.

Les personnes morales sont débitrices de cette obligation à un double niveau. D'une part, et si l'on considère que le droit à l'oubli des données personnelles est opposable *erga omnes*, elles devront s'abstenir de toutes atteintes aux données personnelles des personnes physiques. D'autre part, lorsque les personnes physiques exerceront leur droit à l'oubli, en qualité de responsable du traitement ou de sous-traitants, les personnes morales seront débitrices de l'obligation « d'effacement ». Si la première obligation dépend de la nature du droit à l'oubli, la seconde à l'effet relatif est intégrée à l'article 17 de la proposition de Règlement européen comme un effet consacré du droit.

Cet article prévoit expressément qu'une personne morale puisse faire usage des données personnelles d'une personne physique, en procédant au traitement, en les utilisant ou simplement en les conservant. Dès lors, les personnes physiques exercent leur droit de faire rectifier des données à caractère personnel et disposent d'un droit à l'effacement lorsque la conservation de ces données n'est pas conforme au Règlement. Ce droit doit également être étendu de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques soit sans justification légale obligé de prendre toutes les mesures nécessaires pour que les données soient effacées, y compris par des tiers, sans préjudice des droits de la victime à indemnisation[36].

L'obligation dont est débitrice la personne morale est du fait de cette dernière disposition lourde et difficile à mettre en œuvre.

Autrement dit, dans le projet de Règlement européen, la personne morale est exclusivement envisagée comme débitrice d'un droit à l'oubli[37].

20. Les obligations élargies par le Parlement européen. La proposition de Règlement européen faite par la Commission européenne ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique, par exemple une correspondance ou la tenue d'un carnet d'adresses, qui sont exclusivement personnels ou domestiques et sans but lucratif, donc sans lien aucun avec une activité professionnelle ou commerciale.

De fait, elle ne valait pas non plus pour les responsables du traitement de données ou leurs sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles

---

36 En ce sens, texte de la Commission LIBE du Parlement européen, Considérant 54 : « Afin de renforcer le "droit à l'effacement" dans l'environnement en ligne, le droit à l'effacement des données devrait en outre être étendu de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques sans motif légal, soit tenu de prendre toutes les mesures nécessaires pour procéder à l'effacement de ces données, y compris pas des tiers, sans préjudice du droit de la personne concernée à demander réparation.», adopté par la Résolution législative du Parlement européen du 12 mars 2014.

37 En ce sens : article 17 al. 1 de la proposition de règlement européen : « une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

activités personnelles ou domestiques[38]. La Commission LIBE du Parlement européen a élargi les obligations incombant aux responsables de traitements ou à leurs sous-traitants, qui peuvent de par leur forme juridique être des personnes morales, y compris lorsqu'il s'agit de données à caractère personnel pour des activités personnelles ou domestiques [39].
Ces nouvelles dispositions élargissent donc le champ des obligations des personnes morales débitrices de la protection des données personnelles des personnes physiques[40].

b) La personne morale, débitrice d'une obligation générale de protection des données personnelles des personnes physiques : le principe d'accountability.

21. Le principe d'accountability. Ce principe n'existe pas en tant que tel dans la loi Informatique et Libertés. Il est clairement affirmé dans la proposition de Règlement européen, notamment à l'article 22[41]. La volonté est de mettre en conformité l'entreprise, autour du concept anglais d'accountability, afin qu'elle place la protection des données personnelles au cœur de sa responsabilité. Toutefois, les termes de « responsability » et d' « accountability » ne doivent pas être tenus pour synonymes. L'accountability se traduit plutôt par l'obligation faite à l'entreprise de rendre des comptes sur le traitement des données personnelles. Ainsi, l'accountability se mesure à trois niveaux : par les politiques de l'entreprise, par les procédures mises en place dans l'entreprise et par ses pratiques[42].

---

38 En ce sens, texte de la Commission européenne (COM(2012)0011), Considérant 15: « Le présent règlement ne devrait pas s'appliquer aux traitements de données à caractère personnel effectués par une personne physique, par exemple un échange de correspondance ou la tenue d'un carnet d'adresses, qui sont exclusivement personnels ou domestiques et sans but lucratif, donc sans lien aucun avec une activité professionnelle ou commerciale. Elle ne devrait pas valoir non plus pour les responsables du traitement de données ou leurs sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.».

39 En ce sens, Texte de la Commission LIBE du Parlement européen, LIBE du Parlement européen, Considérant 15 : « Le présent règlement ne devrait pas s'appliquer aux traitements de données à caractère personnel effectués par une personne physique, par exemple un échange de correspondance ou la tenue d'un carnet d'adresses ou une vente privée, qui sont exclusivement personnels, familiaux ou domestiques et sans lien aucun avec une activité professionnelle ou commerciale. Toutefois, le présent règlement devrait s'appliquer aux responsables du traitement de données et à leurs sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques », adopté par la Résolution législative du Parlement européen du 12 mars 2014.

40 Dépassant le cadre de notre étude, nous n'aborderons pas cette question de manière exhaustive. V. toutefois CJUE 13 mai 2014, affaire C-131/12, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González. L'exploitant d'un moteur de recherche sur Internet est responsable du traitement qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers.

41 Selon la Résolution législative du Parlement européen du 12 mars 2014, l'article 22 de la proposition de Règlement est intitulé : « Obligations et responsabilité du responsable du traitement », amendant l'intitulé de l'article 22 proposé par la commission européenne (COM(2012)0011) : « Obligations incombant au responsable du traitement ».

42 Intervention de D. LE METAYER, Quoi de neuf dans le principe d'accountability, peut-il être un instrument vraiment effectif en matière de vie privée ?, Journée INRIA - AFDIT - instruments de protection de la vie privée, 11 septembre 2013. Citant les travaux de Colin BENNETT, International Privacy Standards: can Accountability be Adequate ?, Privacy Laws and Business International, 2010 - colinbennett.ca.

22. La mise en œuvre de l'accountability dans la proposition de Règlement européen. La proposition de Règlement européen édicte toute une série de mesures : l'article 5 le responsable de traitements doit prouver qu'il respecte bien l'ensemble des dispositions du règlement ; les articles 11 et 12, il doit rédiger et appliquer des règles internes transparentes et facilement accessibles en ce qui concerne le traitement des données et en vue de l'exercice de leurs droits par les personnes concernées ; l'article 22 prévoit des audits internes ou externes ; l'article 26, il doit conserver les traces documentaires des instructions données au sous-traitant. Enfin une étude d'impact (« privacy impact assessment ») doit être réalisée sur les traitements mis en œuvre comportant des risques particuliers.
Si les obstacles doctrinaux à la titularité d'un droit à l'oubli ou à l'effacement pour les personnes morales peuvent être levés, les barrières du droit positif restent pour l'heure fermées à ce bénéfice. Les personnes morales sont-elles alors totalement dépourvues de protection à l'égard du traitement de leurs informations à caractère personnel et à la libre circulation de ces informations. Les outils juridiques mis à leur disposition par le droit positif sont-ils suffisamment protecteur de leurs intérêts ? Et si la protection est aujourd'hui suffisante et efficiente ne vide-t-elle pas le débat sur la titularité d'un droit à l'oubli ou l'effacement pour les personnes morales ?

Section 2- L'utilité de la reconnaissance d'un droit à l'oubli pour les personnes morales

23. Questionnement. La titularité d'un droit à l'oubli étant refusée par le droit positif, il est alors possible de s'interroger sur l'opportunité d'élargir ce bénéfice aux personnes morales. En pratique, le responsable du traitement procède à l'effacement des données concernant les personnes physiques sans délai, sauf lorsque la conservation des données à caractère personnel est nécessaire, par exemple pour l'information sur les questions mémorielles.
La personne morale dispose de moyens judiciaires et extrajudiciaires pour obtenir un résultat proche de l'effacement. Elle n'est donc pas dépourvue de ressources pour la protection des informations diffusées la concernant et pourra se défendre contre toute atteinte (II). Il convient toutefois de relativiser l'opportunité de ces outils à l'inconvénient de soumettre la personne morale à la lourdeur et l'exposition médiatique d'un procès, lorsque la solution devient judiciaire. Ajoutons que la protection des informations d'une personne morale se heurte aux atteintes légitimes qui reposent sur un intérêt supérieur, et ce dans un rapport certainement moins équilibré que celui consenti à la protection des données personnelles des personnes physiques. Le moyen le plus efficace alors pour les personnes morales consiste à opérer très en amont une protection de ses informations personnelles et commerciales, en maîtrisant son empreinte numérique (I).

I- Les solutions préventives de protection des informations par les personnes morales

24. De la veille informationnelle à la mort numérique. Puisqu'aucune obligation légale n'impose aux responsables de traitement d'informer la personne morale de la collecte, de l'utilisation ou même de la conservation des informations la concernant, elle doit y procéder par elle-même. Cette veille informationnelle passe par des actions de surveillance (A) et par une présence volontaire de l'entreprise sur Internet, qui peut conduire au déréférencement, autrement dit sur Internet à la « mort numérique » (B). Le droit vient en support de ces pratiques en

proposant aux dirigeants de protéger, hors procédures contentieuses, les informations détenues par les personnes morales (C).

A- Action de surveillance

25. La surveillance, en pratique. Une surveillance efficace permet à la personne morale de ne pas avoir besoin de recourir aux techniques informatiques d'effacement. Autrement dit, il devient préférable de contrôler la diffusion d'informations en amont de leur publication plutôt que de solliciter leur oubli.

En effet, les personnes morales poursuivent un impératif : se construire une image numérique, afin de créer l'influence recherchée. Ainsi lorsqu'une entreprise décide d'investir dans le développement de son image, elle doit veiller à ce que l'information qu'elle véhicule ne puisse pas être altérée[43]. Pour cela, elle peut notamment utiliser des logiciels comme collecteurs d'informations directes ou indirectes (sur les clients, les concurrents, etc.) Le moteur de recherche permet également cette surveillance : soit avec le célèbre le googling qui consiste à rechercher des informations sur google à partir d'un nom ou d'une marque ; soit en automatisant ce travail par le service « Google Alert », qui permet de définir des alertes par mots clés.

D'un côté, la veille s'effectue sur les acteurs de l'entreprise, employés clients ou partenaires. Les dirigeants doivent s'assurer que les accès aux divers comptes de l'entreprise (site institutionnel, pages Facebook ou Twitter...) soient sécurisés au risque de voir de fausses informations diffusées. De nombreuses affaires évoquent des faits de diffamation ou d'injures d'employés envers leurs supérieurs sur les réseaux sociaux écornant plus ou moins publiquement l'image de l'entreprise[44].

D'autre côté, la surveillance porte sur les acteurs d'Internet, qu'ils soient consommateurs[45] ou experts-professionnels. Décrivant le pouvoir des consom-acteurs, un auteur illustre[46] l'impact de l'information diffusée par de simples clics « J'aime » sur un réseau social ou par l'influence générée de bloggers. Autre exemple, avec la société Air France qui surveille 2 500 sources en Europe et en Amérique du Nord sur près d'un millier de mots clés. Sur cette liste, on trouve des termes comme « sonde Pitot » ou « QRF » (Quick Return Flight), le code utilisé par les pilotes pour indiquer leur retour au sol à la suite d'un incident technique[47].

---

43 En ce sens, S. ALLAIRE et H. PHAURE, 3 questions. Le risque de réputation, JCP E n° 41, octobre 2012, 604 : « l'image, qui appréhende le risque de réputation comme l'écart entre l'image émise de l'entreprise - représentation que se donne l'entreprise vis-à-vis d'une partie prenante - et l'image perçue - perception de cette partie prenante »

44 Par exemple : TGI Paris, 17ème ch. corr., 17 janv. 2012, n° 1034008388, condamnant un salarié pour avoir publié des injures publiques sur sa page Facebook dans les termes suivants : « Journée de merde, temps de merde, boulot de merde, boîte de merde, chef de merde... » « Ben j'aime pas les petits chefaillons qui jouent au grand ». Le tribunal a jugé que le passage litigieux comportait « clairement des expressions outrageantes à l'encontre de la direction et de l'entreprise » et excédait « les limites de la critique admissible, y compris lorsqu'elle s'exerce dans un cadre syndical ».
V. aussi : Civ. 1ère, 10 avr. 2013, n° 11-19.530, note B. BOSSU, Le salarié, le réseau social et l'injure, JCP E 2013, n°25, I, 1371 : « Dès lors que les propos litigieux sont diffusés sur des comptes ouverts par un salarié sur le site Facebook et sur le site MSN, accessibles aux seules personnes agréées par l'intéressé, en nombre très restreint, la caractérisation d'une communauté d'intérêts exclut que les propos soient qualifiés d'injures publiques. En revanche, il convient de rechercher si les propos litigieux peuvent être qualifiés d'injures non publiques ».

45 Et aussi, v. infra sur le Droit de la consommation et l'emploi des « faux avis ».

46 ADAMY, Le Web social et la e-réputation, Le nouveau pouvoir des consom-acteurs, op. cit. p. 44

47 S. LUPIERI, Comment les entreprises soignent leur e-réputation, Les échos, 3 avril 2013.

Pour répondre à ces objectifs, de nouvelles fonctions sont apparues : chargés de communication web, *webmarketeur*... Ces prestations sont soit internalisées soit externalisées par l'entreprise. Le contrat qui organise ses relations et surtout l'objet de la prestation doit être particulièrement soigné[48].

B- La présence volontaire

26. Les techniques de référencement naturel vers le déréférencement. La présence volontaire se manifeste par les techniques de référencement naturel[49]. L'entreprise qui décide d'optimiser la visibilité de son site Internet dispose de plusieurs moyens dont notamment le référencement sur des moteurs de recherche. Elle peut alors améliorer son positionnement, même si l'indexation des sites internet dans les moteurs de recherche est réalisée de façon automatique. Elles emploient des techniques dites de « référencement naturel », qui par des algorithmes confidentiels et évolutifs évaluent automatiquement la pertinence d'un site internet en fonction des mots clés saisis par un internaute dans le moteur de recherche. Il est donc nécessaire de connaître ces algorithmes pour agir sur le positionnement d'un site.
L'entreprise qui souhaite ainsi enfouir certaines informations la concernant, afin que ces informations ne soient plus accessibles au public, pourra agir en vue d'un déréférencement. Il s'agit en pratique de définir le nombre de pages que l'entreprise souhaite interposer devant le lien négatif. Le déréférencement total de l'entreprise sur Internet conduit à sa « mort numérique ». Ce déréférencement a une portée pratique équivalente à la mise en œuvre d'un droit à l'effacement, comme prévu par la proposition de règlement européen[50], même si techniquement il s'agit plus « d'écrasement » que « d'effacement ».

C- Les solutions juridiques préventives

27. La solution amiable. Lorsqu'une entreprise est victime d'un message au contenu illicite, elle peut engager la responsabilité des hébergeurs dès lors qu'ils avaient connaissance de ce caractère illicite. Pour cela, l'entreprise doit notifier un certain nombre d'éléments et d'informations, dans les formes prescrites par l'article 6-I-5° de la loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique (LCEN). La notification de l'article 6-I-5° répond à des exigences formelles précises, qu'il convient de respecter impérativement. Parfois, une simple mise en demeure par voie d'avocat s'avère efficace et le contenu illicite est supprimé par « nombre d'hébergeurs pratiquant le principe de précaution »[51]. Même si elle ne permet pas de sanctionner l'auteur du contenu illicite, cette solution amiable est souvent préférée.

---

48 Question sur la réversibilité du contrat, sur la propriété des bases de données qui ont découlé de la surveillance, de l'étendue des obligations de surveillance, sont autant d'enjeux de la rédaction de ces nouveaux contrats.

49 Sur cette question, v. notamment l'article de A. FIÉVÉE et C. MARTIN, L'« e-réputation » : la gestion juridique de l'image de l'entreprise sur internet, RLDI 2011, n°72, p. 70.

50 V. infra.

51 F. HERPE, L'atteinte à la réputation d'une personne physique ou morale sur internet, RLDI 2010, n°27, p. 67.

28. Le droit de réponse. Le droit de réponse consiste à pouvoir solliciter du Directeur de publication l'insertion d'une réponse à des informations divulguées dans des journaux ou périodiques (article 13 de la loi du 29 juillet 1881). Ce droit de réponse a été ouvert par la LCEN (article 6-IV, al. 1er) pour les services de communication au public en ligne qui « permet à une personne qui a été citée dans un média de soumettre au média en question un droit de réponse sur le même support qu'il aura l'obligation de publier ». Le droit de réponse est ouvert aux personnes morales, puisque le texte de la loi sur la presse indique « les réponses de toute personne nommée ou désignée dans le journal ou écrit périodique ». L'exercice du droit de réponse n'impose aucune condition (contenu diffamatoire ou information erronée) et la demande doit être présentée dans un délai de trois mois.
Est-ce que ce droit de réponse se substitue dans ses effets à un effacement ? On peut en douter. La volonté de contredire avec plus ou moins de véhémence toute référence à une atteinte et notamment si elle a lieu sur internet peut provoquer le résultat inverse de celui escompté. Les spécialistes appellent cela « l'effet Barbra Streisand». À l'époque, l'artiste avait fait interdire par décision de justice une photo aérienne de sa maison publiée sur internet. Le résultat a été la diffusion à grande échelle de l'image et de vives critiques des internautes contre la chanteuse. Par analogie, dans le milieu industriel existe « l'effet Nestlé ». En mars 2010, Greenpeace publie sur *You Tube* une vidéo parodique d'une publicité pour la barre chocolatée *KitKat*, qui contient de l'huile de palme. Greenpeace a alors mis en scène les conséquences désastreuses de l'exploitation de l'huile de palme sur l'habitat des orangs-outangs. Nestlé a sollicité la suppression de de la vidéo et menace les internautes de supprimer leurs messages, mais a offert par ricochet une meilleure tribune à Greenpeace[52].

29. Le droit des procédures collectives. Au terme de l'article R. 626-20 du code de commerce, la société peut obtenir la radiation d'office de toute mention au RCS d'une procédure de sauvegarde ou de redressement judiciaire, dès lors que le plan est toujours en exécution au terme d'un délai de trois ans à compter de son arrêté pour la première mention, et de cinq ans pour la seconde[53]. Ce texte est une aide à l'entreprise qui a montré sa capacité à se réorganiser. La condition de délai permet de préserver le nécessaire droit à l'information des tiers, plus précisément des créanciers, sur la situation financière de l'entreprise.
Une telle radiation fait obstacle à toute nouvelle mention intéressant l'exécution du plan de sauvegarde ou de redressement, sauf si celle-ci est relative à une mesure d'inaliénabilité décidée par le tribunal ou à une décision prononçant la résolution du plan.

II- Les solutions répressives de protection des informations par les personnes morales

30. Des actions différentes aux effets similaires ? La personne morale ne bénéficiant des solutions législatives au droit à l'oubli, à la rectification, à l'opposition ou à l'effacement peut

---

52 Sur cette affaire, v. notamment : G. ADAMY, Le Web social et la e-réputation, Le nouveau pouvoir des consom-acteurs, op.cit. p. 64-65.

53 Décret n°2011-1836 du 7 décembre 2011, relatif aux radiations d'office du registre du commerce et des sociétés en matière de plans de sauvegarde et de redressement. V. notamment P. ROUSSEL GALLE, Droit à l'oubli…du moins au RCS… Revue des sociétés, 2012, p. 188.

toutefois obtenir par des moyens judiciaires une sanction d'un contenu qui lui porterait atteinte. Dans un premier temps, nous dresserons un inventaire des différentes actions qui permettent à une personne morale de protéger judiciairement ses informations (A). Dans un second temps, nous étudierons si les sanctions ouvertes par ces différentes actions peuvent produire des effets similaires aux sanctions accordées aux personnes physiques pour obtenir l'effacement, voire une forme d'oubli (B).

A- Les actions ouvertes aux personnes morales pour la protection de leurs informations

31. La qualification des atteintes et la légitimité de l'effacement. Cybersquatting, faux profils sur les forums ou les réseaux sociaux, dénigrement, atteinte aux marques, usurpation d'identité, diffamation et injures… voici un panel d'atteintes dont peut être victime une entreprise et qu'elle souhaiterait voir sanctionner, afin d'en obtenir le retrait sur internet. Telle est alors la grande différence avec les personnes physiques. Les personnes morales sont soumises au contrôle du juge sur la réalité du dommage pour légitimer leur demande d'effacement, voire d'oubli. Elles peuvent à cet effet actionner les droits fondamentaux (a), le droit de la responsabilité (b) et le droit pénal (c).

a) Le recours aux droits fondamentaux

32. L'intérêt des droits fondamentaux. La personne morale peut actionner des droits et libertés fondamentaux afin de sanctionner les atteintes causées par des tiers à son image numérique. Le principe même de la reconnaissance des droits fondamentaux des personnes morales dépasse le cadre de cette étude[54]. Il a été souligné que « dans le silence des textes, l'affirmation de droits fondamentaux des personnes morales est d'abord imputable aux juges »[55]. En ce sens, ils ont récemment fondé une action visant à protéger la réputation commerciale d'une entreprise. Dans l'affaire jugée par la CEDH le 19 juillet 2011[56], Peter Uj, un journaliste hongrois se plaint d'une violation de son droit à la liberté d'expression du fait d'une condamnation pour diffamation. Le requérant avait vivement critiqué dans un article de journal la qualité d'un vin produit par une entreprise d'État. Les juridictions nationales admettent son droit à la critique, mais non l'insulte gratuite atteignant de manière injustifiée le droit du producteur de jouir d'une bonne réputation. La Cour a alors jugé qu'« il y a une différence entre une atteinte à la réputation d'une personne physique, qui peut avoir des répercussions sur la dignité de celle-ci, et une atteinte à la réputation commerciale d'une société, laquelle n'a pas de dimension morale ».

33. L'apport des droits fondamentaux. De par la formulation employée, la Cour aurait pu conclure que par comparaison à la réputation d'un individu celle dite commerciale est peu

---

54 Et a fait l'objet d'une démonstration en trois parties de X. DUPRE de BOULOIS, Les droits fondamentaux des personnes morales : 1ère partie, RDLF 2011, chron. n°15 ; 2ème partie, RDLF 2011, chron. n°17 ; 3ème partie, RDLF 2012, chron. n°01.

55 X. DUPRE de BOULOIS, Les droits fondamentaux des personnes morales, 2ème partie, RDLF 2011, chron. n°17

56 CEDH, 19 juill. 2011, n° 23954/10, Uj c/ Hongrie. Confirmant l'arrêt CEDH, 15 févr. 2005, n° 68416/01, Steel et Morris c/ Royaume-Uni

importante et que le niveau de sa protection sera faible. La Cour s'était prononcée en ce sens dans l'arrêt Steel Morris en 2005 : « les grandes entreprises s'exposent inévitablement et sciemment à un examen attentif de leurs actes et, de même que pour les hommes et les femmes d'affaires qui les dirigent, les limites de la critique admissible sont plus larges en ce qui les concerne »[57]. L'apport de la décision Uj c/ Hongrie dépasse cette problématique de la hiérarchisation du niveau de protection entre personnes physiques et personnes morales. Elle permet d'envisager de manière autonome les droits fondamentaux des personnes morales. En effet, en leur niant le recours au concept de dignité réservé à la personne humaine, elle invite à une construction qui ne sera pas le décalque de celle appliquée aux personnes physiques, une construction propre qui répond mieux aux spécificités de leur personnalité. Ainsi, la réputation qui contribue au « succès commercial et la viabilité des entreprises pour le bénéfice des actionnaires et des employés, mais aussi pour le bien économique au sens large »[58] devient un intérêt *conventionnalisé* concurrent à ceux protégeant la liberté d'expression et la liberté des débats.

Dans sa thèse consacrée aux fondamentaux des personnes morales, R. Pierre a démontré qu'il était possible de classer les droits fondamentaux en considération de leurs spécificités[59]. Il distingue les droits matriciels à la personne morale (relatifs à leur personnalité juridique), les droits fondamentaux accessoires à l'existence de la personne morale (ex. droit de propriété) et les droits sociaux conditionnés par l'objet social du groupement (ex. liberté d'association). En notre cas, la sollicitation d'effacement d'information permettant de construire une réputation commerciale positive est le moyen pour la personne morale de « réaliser son objet social », une de ses spécificités[60]. L'objet social est traditionnellement défini en rapport avec l'article 1832 du Code civil, à savoir la mise en commun des biens ou d'activité en vue de partager le bénéfice ou l'économie qui en résulte. Il décrit en pratique le genre d'activité que la société se propose d'exercer[61]. L'objet social détermine l'étendue des droits conférés aux personnes morales.

34. Le fondement conventionnel d'un droit des personnes morales sur leurs informations commerciales. La décision Uj c/ Hongrie conduit à s'interroger sur le fondement sur lequel les personnes morales pourraient agir. En notre espèce, la décision a été rendue sur la base de l'article 10 de la Convention protégeant la liberté d'expression du requérant. Tel était aussi le fondement de la requête dans l'arrêt Steel Morris de 2005. La Cour met en balance un certain nombre de facteurs lorsqu'elle apprécie la proportionnalité de la mesure incriminée. Nous ne les reprendrons pas ici, mais nous remarquons que le juge apprécie la proportionnalité de l'ingérence dans la liberté d'expression à l'aune de la « protection de la réputation ou des droits d'autrui », sans fonder cette dernière. Récemment, la Chambre sociale de la Cour de cassation n'a

---

57 CEDH 21 septembre 1994, Fayed c. Royaume-Uni, série A no 294-B, p. 53, § 75, cité par CEDH, 15 févr. 2005, n° 68416/01, Steel et Morris c/ Royaume-Uni.

58 CEDH, 15 févr. 2005, n° 68416/01, Steel et Morris c/ Royaume-Uni.

59 R. PIERRE, Les droits fondamentaux des personnes morales de droit privé, Limoges, 2010.

60 Sur cette question, v. DUPRE de BOULOIS, Les droits fondamentaux des personnes morales, 2ème partie, RDLF 2011, chron. n°17

61 Ph. MERLE, Droit commercial, Sociétés commerciales, 16e éd. Dalloz, Précis, 2013, p. n°52 p. 81.

pas laissé transparaître d'indice sur un fondement à la protection de la réputation commerciale[62]. S'inscrivant dans la lignée des arrêts européens précités, elle a apporté des restrictions à la liberté d'expression d'un salarié ayant conclu une transaction après la rupture de son contrat de travail afin d'assurer la protection de la réputation de l'entreprise employeur et des droits d'autrui.

S'il s'agit d'une première étape vers l'autonomisation d'un droit à la réputation commerciale, il serait alors nécessaire de justifier son rattachement à une disposition conventionnelle. Si une personne morale souhaite agir en défense de sa réputation commerciale du fait de l'emploi par un tiers des informations personnelles et commerciales la concernant, l'article le plus propice ne serait pas nécessairement l'article 8 de la Convention, même s'il a déjà été appliqué aux personnes morales[63]. En effet, l'article 8 a servi de fondement à la protection de la réputation d'une personne physique, considérant : « la réputation d'une personne représente une partie de son identité personnelle et psychique, qui relève de sa vie privée »[64]. L'analogie avec les personnes morales est ici peu satisfaisante. L'article 11 de la CEDH, qui garantit la liberté d'association, pourrait plus justement fonder la protection de la réputation commerciale d'une personne morale[65]. En effet, l'article 11 protège l'existence des personnes morales en ce qu'elles puissent mener librement leurs activités, c'est à dire « la poursuite des divers buts sociaux ou économiques »[66]. Parmi ces buts sociaux et économiques, la personne morale pourra faire valoir la protection de ses informations personnelles et commerciales qui concourent à former sa réputation commerciale et qui lui permettent la réalisation de son objet social.

b) L'engagement de la responsabilité

35. La responsabilité générée par une faute et motivé par un préjudice. L'utilisation des informations personnelles ou commerciales d'une entreprise peut constituer d'une part une faute susceptible de causer un préjudice, sanctionnée sur le fondement de la responsabilité de droit commun ou sur le fondement de régimes spéciaux de responsabilité.

36. Choix d'un régime commun ou spécial de responsabilité. Il existe plusieurs fondements pour engager la responsabilité d'un prestataire ou d'un concurrent qui utiliserait à mauvais escient les informations personnelles ou commerciales d'une personne morale. Le principal intérêt de la responsabilité de droit commun est d'offrir des délais de prescription pour des actes qui notamment seraient affectés par la courte prescription de la loi sur la presse (loi de

---

62 Soc, 14 janvier 2014, 12-27.284, P. d'A. c/ SA Télévision Française 1 (TF1) : JurisData n° 2014-000207 ; comm. J.-B. PERRIER, La transaction, le juge et la restriction de la liberté d'expression de l'ancien salarié, JCP E, 2014, n°19, p. 1259.

63 CEDH, 30 mars 2004, n° 53984/00, Radio France et a. c/ France, RTD civ. 2004, p. 801, obs. J.-P. Marguénaud ; D. 2004, p. 801, obs. C. Birsan. : « le droit à la réputation figure parmi les droits garantis par l'article 8 de la Convention, en tant qu'élément de la vie privée ».

64 CEDH, 14 oct. 2008, n° 78060/01, Petrina c/ Roumanie, JCP G 2009, I, 104, obs. F. Sudre ; RTD civ. 2008, p. 648, obs. J.-P. Marguénaud.

65 En ce sens, R. PIERRE, La protection européenne du droit à la réputation : de la nécessaire distinction entre personne physique et personne morale, CCE n° 5, mai 2012, étude 10.

66 CEDH, 27 mars 2008, n° 26698/05, Tourkiki Enosi Xanthis et a. c/ Grèce, § 43.

1881)[67]. Or, c'est le choix de la juste qualification des pratiques qui pose aujourd'hui le plus de difficulté lorsqu'une action est menée sur le fondement de la responsabilité civile de droit commun. La jurisprudence relève en la matière de la casuistique. Il est toutefois admis depuis un arrêt de l'assemblée plénière de 2000 que les abus de la liberté d'expression prévus et réprimés par la loi du 29 juillet 1881 ne peuvent être réparés sur le fondement de l'art. 1382 C. civ[68]. En d'autres termes, et si l'on prend l'exemple de propos dénigrants, s'ils visent une personne physique ou une personne morale, ils relèvent de la loi sur la presse, et s'ils visent les produits ou services d'une entreprise, ils relèvent de la responsabilité de droit commun. Le régime de la responsabilité civile de droit commun, fondé sur l'article 1382 du Code civil permet de sanctionner les actes de concurrence déloyale. Ainsi la collecte, l'utilisation ou même de la conservation des informations concernant les personnes morales peuvent devenir fautives et constituer des pratiques de dénigrement par des propos mensongers ou exagérés, des captations de clientèle par des procédés déloyaux ou encore du débauchage de salariés.

La responsabilité civile comporte une autre facette, qui est celle du parasitisme. La distinction concurrence déloyale et parasitisme est aujourd'hui désuète, puisque l'exigence d'un rapport de concurrence est assouplit. Il n'empêche que la notion de parasitisme est fortement attachée à celle de « notoriété » ou de « réputation », tel que l'exprimait le père du parasitisme M. Yves Saint Gal : « l'agent fautif vit en parasite dans le sillage d'un autre en profitant des efforts qu'il a réalisés et de la réputation de ce son nom et de ses produits ». La Cour d'appel a récemment sanctionné sur ce fondement la reprise des conditions générales de vente présentées sur le site internet d'une célèbre société de vente à distance[69]. Il ressort de cet arrêt que l'entreprise engage sa responsabilité non par la simple reprise du travail d'autrui, mais lorsqu'il y a captation de la réputation d'autrui à travers la reprise de son travail.La faute est alors constituée notamment par des actes de dénigrements, qui prennent la forme de propos mensongers ou disproportionnés et qui consistent par exemple à jeter le discrédit sur un concurrent en diffusant sur lui, ou au sujet de ses produits ou services, des informations malveillantes. Une des principales limites à la reconnaissance d'un comportement fautif est la liberté d'expression. Les restrictions à ce droit fondamental sont appréciées en considération de la qualité de l'auteur des propos. En effet, des consommateurs ou un organe d'expression collective bénéficient d'une liberté d'expression plus étendue que les salariés ou les concurrents d'une entreprise. Les parodies de grandes marques offrent de nombreuses illustrations, qu'elles émanent des internautes ou d'organisations instituées telles que Greenpeace, avec notamment les affaires Areva, Esso ou encore Nestlé[70]. Outre les facteurs classiques de proportionnalité, il est vérifié par le juge que l'organe d'expression collective agît correctement dans les limites de son objet statutaire ou social, et ce dans un but d'intérêt général. Quant aux parodies, réalisées à des fins humoristiques, elles doivent répondre aux critères habituels pour ne pas tomber sous le coup d'une responsabilité à savoir : ne pas créer

---

67 V. infra sur la diffamation.

68 Cass. ass. Plén., 12 juill. 2000, D. 2000. Somm. 463, obs. Jourdain ; RTD civ. 2000. 842, obs. Jourdain ; ibid. 845, obs. Jourdain ; Légipresse, oct. 2000, n° 75, concl. M. le Premier avocat général Joinet.

69 Cour d'appel de Paris, le 24 septembre 2008, arrêt Vente.privée.com c/ Kalypso.

70 Paris, 4e ch. B, 17 nov. 2006 (affaire Areva) ; Paris, 4e ch. A, 16 nov. 2005, n° 04/12417 (Affaire Esso), observations P. TREFIGNY, La libre critique des marques, Chronique Droit du numérique, D. 2007, p. 1191 ; C. GEIGER, Droit des marques et liberté d'expression, de la proportionnalité de la libre critique, D. 2007. Chron. 884.

de confusion entre l'œuvre et la réalité et ne pas laisser un internaute moyen croire que la parodie réelle. Le préjudice réparable au titre des atteintes aux informations souvent commerciales d'une personne morale est pour l'essentiel des chefs de préjudice d'ordre économique. Tel est le cas de la perte de clientèle[71], laquelle se manifeste dans le *lucrum cessans*, ou encore du manque à gagner.

Toutefois, les atteintes aux informations commerciales d'une entreprise ne sont pas seulement de nature patrimoniale. Se pose alors la question de l'indemnisation du préjudice moral d'une entreprise sociétaire. Il est depuis longtemps admis que l'intégration du préjudice moral au titre des sommes réparables peut se faire sur le fondement de la concurrence déloyale. Cela a été rappelé lors d'un arrêt récent[72], fort mal rédigé, mais très explicite, indemnisant une société « La pizzeria » de son préjudice moral, qui dépoussiéra le débat sur le déjeuner avec une personne morale. Il n'est dès lors pas question d'attacher à l'indemnisation du préjudice moral de la personne morale le sens traditionnel du sentiment ou de la souffrance, mais de rechercher les atteintes à son identité propre, sa culture, ses valeurs, ses emblèmes ou son image.

37. Les régimes spéciaux de responsabilité. Le droit des marques. L'utilisation d'une marque n'est possible qu'après avoir recueilli le consentement préalable de son titulaire (article L. 713-1 et L. 713-2 du Code de la propriété intellectuelle, même si la reproduction ne s'accompagne pas d'un usage commercial). Par exemple, peut être sanctionnée l'utilisation de la marque comme mot clé, *métatag* afin d'obtenir un meilleur référencement sur Internet et générer un lien désignant les produits et services identiques ou similaires à ceux désignés dans l'enregistrement[73]. De même, employer le signe distinctif d'une entreprise pour exprimer un message sur Internet ne constitue pas en soi un acte de contrefaçon. En effet, le contrefacteur présumé doit avoir utilisé le signe dans la vie des affaires, c'est-à-dire dans le cadre « d'une activité commerciale visant à un avantage économique et non dans le domaine privé »[74]. Le juge par un faisceau d'indices recherche si le message s'inscrit dans le cadre de la vie des affaires ; si il émane d'un concurrent ; s'il y a un risque de confusion avec la marque ou les produits d'un concurrent et enfin, s'il y a dénigrement de la marque ou des produits de l'entreprise. Il apprécie également le message au regard du respect dû

---

71 Encore faut-il démontrer par le demandeur la preuve que les clients et prospects avaient été détournés sous l'action de son concurrent, in T. Com. Montpellier 17 janvier 2011, Partenaire Européen / AK associés, http:/www.legalis.net.

72 Com., 15 mai 2012, Société La Pizzeria contre Monsieur et Madame Fournier, n°11-10.278 : D. 2012. 2285, obs. X. DELPECH, note B. DONDERO ; ibid. 2688, obs. J.-C. HALLOUIN, E. LAMAZEROLLES et A. RABREAU ; Rev. sociétés 2012. 620, note P. STOFFEL-MUNCK ; RTD civ. 2013, p. 81, obs. J. HAUSER, On ne peut déjeuner avec une personne morale, mais elle pourrait en souffrir !; JCP E 2012, n°36, p. 29, note R. MORTIER, Reconnaissance par la Cour de cassation du préjudice moral d'une société ; RLDA 2012, n°74, p. 10, note B. MARPEAU et M. NEZAM ; Rev. dr. des sociétés 2012, n°9, p. 19 obs. R. MORTIER.

73 En ce sens, contribution de P. TREFIGNY, Colloque du CUERPI, 6 décembre 2013, L'entreprise à l'épreuve du droit de l'Internet, Quid novi ?, contribution sur Liens commerciaux et droit des marques, actes à paraître.

74 Com., 10 mai 2011, n° 10.18.173, Bull. civ. IV, n°72. Sur l'aspect privé (hors de la vie des affaires) de l'utilisation d'une marque sur les réseaux sociaux, v. notamment A. MARIE, C. GHASSEMI, G. VEDEL, Contrefaçon de marques et e-réputation sur les réseaux sociaux : les nouveaux défis des titulaires de marques, RLDA, 2013, n°87, p. 106.

à la liberté d'expression et de la nécessité de préserver des débats d'intérêt général[75]. Suivent ces incriminations les pratiques de *cybersquatting, typosquatting, pornsquatting*[76] ou de parodie[77].

38. Les régimes spéciaux de responsabilité. Le secret des affaires. Actuellement, la violation du secret des affaires ne constitue pas une infraction, que cela soit sur internet ou ailleurs. Les mesures financières imposées en cas de violation du secret des affaires ont vocation à réparer le préjudice causé, mais pas à réprimer l'acte lui-même. Ce sont des récentes affaires, telles que Wikileaks, de vols de secret d'affaires médiatisées qui ont mis en évidence la fragilité de nombreuses entreprises. D'ailleurs la perte de confiance liée à un effondrement de l'image peut même aller jusqu'à entraîner la disparition de l'entreprise quel que soit sa taille, comme dans le cas de Arthur Andersen (affaire Enron, destruction des documents...). Le 23 janvier 2012, l'Assemblée nationale avait adopté en première lecture une proposition de loi visant à sanctionner pénalement la violation du secret des affaires[78]. S'inspirant du Cohen Act américain, qui a érigé la divulgation de secrets des affaires en crime fédéral, elle constituait une avancée significative pour une protection plus efficace du secret des affaires. En effet, la valeur économique de l'information procède de son caractère secret et, par voie de conséquence, de l'avantage concurrentiel qu'elle peut procurer. Cette nouvelle infraction permettait donc de protéger les informations, parfois sensibles. Cependant, la définition ne visait que la révélation d'un secret des affaires, ce qui s'avère pour le moins restrictif, rendant son application compliquée[79]. En effet, ce texte prévoyait l'introduction d'un nouvel article 325-1 du Code pénal ainsi rédigé : « Constituent des informations protégées relevant du secret des affaires d'une entreprise, quel que soit leur support, les procédés, objets, documents, données ou fichiers de nature commerciale, industrielle, financière, scientifiques, technique ou stratégique ne présentant pas un caractère public dont la divulgation non autorisée serait de nature à compromettre gravement les intérêts de cette entreprise en portant atteinte à son potentiel scientifique et technique, à ses positions stratégiques, à ses intérêts commerciaux ou financiers ou à sa capacité concurrentielle et qui ont, en conséquence, fait l'objet de mesures de protection spécifiques destinées à informer de leur caractère confidentiel et à garantir celui-ci ». La sanction prévue était de 3 ans d'emprisonnement et 375 000 euros d'amende. Toutefois, la poursuite du processus législatif semble interrompue depuis les élections présidentielles et législatives.

---

75 En ce sens, v. notamment : TGI Paris, réf., 4 avr. 2013, n°13-52578, SAS H&M Hennes & Mauritz Logistics GBC France, H&M Hennes & Mauritz c/ Google, Youtube LLC : « le signe reproduit sur leurs sites Internet ne vise pas plus à désigner qu'à promouvoir un produit qui serait offert à la vente, mais seulement à informer l'internaute du comportement éventuel de la société titulaire de la marque en question, de sorte qu'il n'a pas pour but de renseigner le consommateur sur la nature ou l'origine d'un produit et n'est nullement utilisé dans la vie des affaires ».

76 Cette pratique consiste à utiliser sans autorisation des noms de domaine contenant une marque pour du contenu pornographique. V. notamment : OMPI, centre d'arbitrage et de médiation, 24 févr. 2013, n° D2012-2422, cité par L. MARINO, Un an de propriété industrielle dans les technologies NBIC . - (nanotechnologies, biotechnologies, technologies de l'information et sciences cognitives), Propriété industrielle n° 3, Mars 2014, chron. 2.

77 Notamment dans le célèbre arrêt : « je boycottedadone.com » (CA Paris, 4ème ch, 30 avril 2003, RG 2001/14371)

78 http://www.assemblee-nationale.fr/13/ta/ta0826.asp. V. aussi l'importante contribution de J.-M. GARINOT, Le secret des affaires, LexisNexis, 2013.

79 D'ailleurs, la poursuite du processus législatif semble interrompue depuis les élections présidentielles et législatives.

Au niveau européen, le 28 novembre 2013, un projet de directive a été proposé par la Commission européenne[80] pour créer une définition commune du secret d'affaires et mettre en place des moyens permettant aux victimes de l'appropriation illicite d'un tel secret d'obtenir réparation. Les juridictions nationales auront un traitement uniforme des affaires d'appropriation illicite d'informations commerciales confidentielles et pourront demander le retrait du marché des produits qui constituent une atteinte à un secret d'affaires et l'octroi de dommages-intérêts. Cette proposition de directive a été adoptée par le Conseil de l'Union européenne, le 26 mai 2014.

Enfin, souhaitant doter le secret des affaires d'un cadre civil, le 16 juillet 2014 une proposition de loi, relative à la protection du secret des affaires a été déposée à l'Assemblée Nationale. Elle se décline en six articles ; le premier d'entre eux a pour objectif de créer, au sein du livre premier du code de commerce, un titre V intitulé « Du secret des affaires » et composé de neuf articles (L. 151-1 à L. 151-9). La définition retenue du secret des affaires est la suivante : « Est protégée au titre du secret des affaires, indépendamment de son incorporation à un support, toute information : « 1° Qui ne présente pas un caractère public en ce qu'elle n'est pas, en elle-même ou dans l'assemblage de ses éléments, généralement connue ou aisément accessible à une personne agissant dans un secteur ou un domaine d'activité traitant habituellement de ce genre d'information ; « 2° Qui, notamment en ce qu'elle est dénuée de caractère public, s'analyse comme un élément à part entière du potentiel scientifique et technique, des positions stratégiques, des intérêts commerciaux et financiers ou de la capacité concurrentielle de son détenteur et revêt en conséquence une valeur économique ; « 3° Qui fait l'objet de mesures de protection raisonnables, compte tenu de sa valeur économique et des circonstances, pour en conserver le caractère non public ». Et la sanction de toute atteinte est l'engagement de la responsabilité civile de son auteur, mais également des mesures pénales de protection du secret des affaires sont expressément prévues à l'article L. 151-8 du Code de commerce.

c) Le recours au droit pénal

39. La loi sur la presse – les difficultés liées à la courte prescription. La loi sur la presse permet de réprimer les utilisations d'informations relatives à une personne morale qui constitueraient une diffamation publique (al.1)[81] et l'injure publique (al.2)[82] au sens de l'article 29 de la loi du 29 juillet 1881[83]. D'après l'article 6-V de la loi n° 2004-575 du 21 juin 2004 pour la

80 Proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, 28 novembre 2013 (COD 2013/0402)

81 Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés.

82 Toute expression outrageante, terme de mépris ou invective qui renferme l'imputation d'aucun fait est une injure.

83 Il est de jurisprudence constante que les faits de diffamation et d'injure s'ils sont caractérisés ne peuvent pas être poursuivis devant les juridictions civiles sur le fondement de la responsabilité civile délictuelle en vue d'obtenir une simple réparation financière. Pour y parvenir, il est donc obligatoire d'initier une procédure pénale (Ass. Plen. 12 juillet 2000, Bull. civ. n°8). Sur cette question, v. M. PICHON de BURY, Internet, Comment lutter contre les atteintes à l'e-réputation ? Expertises, octobre 2012, p. 343.

confiance en l'économie numérique, les dispositions des chapitres IV et V de la loi du 29 juillet 1881 précitées sont applicables aux services de communication au public en ligne et la prescription acquise dans les conditions prévues par l'article 65 de ladite loi. La prescription de l'assignation est de trois mois en matière de délits de presse à compter de la mise en ligne. Deux difficultés sont apparues dans l'application de la loi du 29 juillet 1881 sur la liberté de la presse aux délits perpétrés sur Internet : celle liée au court délai de prescription ayant pour conséquence la nullité de l'assignation (article 53) et celle liée à l'identification de l'auteur de l'infraction[84]. Les personnes morales peuvent être victimes d'une diffamation ou d'une injure[85].

40. La loi sur la presse – Google Suggest. Récemment, la Cour de cassation le 19 juin 2013 a eu à se prononcer sur la demande d'une personne morale dans la suppression des suggestions attentatoires à ses intérêts réalisées par Google[86]. *Google Suggest* est un outil d'aide à la recherche sur internet, qui offre aux internautes effectuant une recherche, à partir des premières lettres du mot qu'ils saisissent, un menu déroulant de propositions qui comporte une liste de requêtes possibles. Ce service de « prévision de recherche » permet aux utilisateurs de profiter de l'expérience des autres. En l'espèce, il était question d'une requête sur le moteur de recherche Google qui aux termes «Lyonnaise de g » laissait apparaître comme suggestion d'aide à la recherche le terme d'« escroc ». La Cour a décidé que : « le rapprochement critiqué n'est que le fruit d'un processus purement automatique dans son fonctionnement et aléatoire dans ses résultats, de sorte que l'affichage des mots-clés qui en résulte est exclusif de toute volonté de l'exploitant du moteur de recherche d'émettre les propos en cause ou leur conférer une signification autonome au-delà de leur simple juxtaposition et de leur seule fonction d'aide à la recherche ». L'action intentée sur le fondement de la loi de 1881, n'a pas donc abouti au motif que « l'intention coupable ne peut se déduire de la mise en œuvre d'un procédé automatisé qui puise parmi les nombreuses requêtes d'internautes afin de faciliter les recherches sur internet sans intervention volontaire de la part du moteur de recherche »[87].

Et pourtant, les arguments de l'exploitant du moteur de recherche qui ont prospéré en 2013 n'ont pas toujours trouvé un accueil favorable dans prétoires. Par exemple, en 2012, la société Kriss Laure[88] était associée au mot « secte » aux troisième et deuxième rangs des dix suggestions de recherche proposées aux internautes. Les juges du fond ont retenu la qualification d'injure (au

---

84 Sur cette seconde difficulté que nous n'aborderons pas dans le cadre de cette étude, v. notamment : E. BAILLY, L'entreprise face aux risques informatiques : les réponses du droit pénal, RLDA 2011, n°64, in Dossier spécial : le risque pénal de l'entreprise : approche pratique des évolutions actuelles.

85 Crim., 12 oct. 1976, no 75-90.239 , Bull. crim., n°287

86 Civ. 1re, 19 juin 2013, n° 12-17.591, Lyonnaise de garantie c/ Google Inc., Google France et M. X : v. not. D. 2013. 1614 ; CCE septembre 2013. Comm. 94 et JCP G 2013, I, 1568 comm. A. LEPAGE ; Legipresse septembre 2013, p. 491, note F. KLEIN et M. BOURGEOIS ; JCP E 2013, n°35 p. 41 A. ZOLLINGER ; RLDI 2013, n°96, p. 63, note E. DERIEUX.

87 P. TREFIGNY, Chronique Droit du numérique septembre 2012 - septembre 2013, sous la direction de J. LARRIEU et P. TREFIGNY, D. 2013, p.2487.

88 TGI Paris, 17e ch., 15 févr. 2012, Kriss Laure c/ Google Inc : CCE mai 2012, comm 50, note G. LOISEAU, Requêtes suggérées ou associées : une menace pour l'e-réputation des entreprises ; CCE mai 2012, comm. 57, obs. A. LEPAGE, Fonctionnalité « Google Suggest » : qualification d'injure retenue.

sens de l'article 29 de la loi de 1881) niant « la neutralité technologique prétendue dudit service » et considérant que les propositions de recherche étaient « de nature à orienter la curiosité ou à appeler l'attention sur le thème proposé et, ce faisant, de nature à provoquer un « effet boule de neige » d'autant plus préjudiciable à qui en fait l'objet que le libellé le plus accrocheur se retrouvera ainsi plus rapidement en tête de liste des recherches proposées ».

Au-delà du caractère automatique de la suggestion de recherche, c'est la volonté de nuire qui est étudiée par les juges, qu'il s'agisse de l'intention de l'exploitant du moteur de recherche ou de celle d'un utilisateur. Comme l'illustre la décision de la Cour d'appel de Lyon du 29 janvier 2013[89] : « la rémanence des données qui persistent malgré les tentatives d'effacement ou de suppression ne saurait constituer en elle-même un acte volontaire de la part de la société Aphysio », qui après son retrait du groupe Avipur s'était vue notifier l'obligation de ne plus faire mention de la dénomination de son ancienne parente. Elle n'est dès lors pas jugée responsable de la persistance de son ancienne association dans les moteurs de recherche. Une sorte de « fatalité technique qui s'imposerait à nous »[90] et pour laquelle le moteur de recherche dispose néanmoins des « moyens d'éviter cette rémanence des données et qui ne devrait pas être autorisé à se réfugier derrière le caractère « automatique » du mécanisme qu'il met en place »[91].
Notons que la qualification retenue soit l'injure ou la diffamation, les demandeurs se heurteront nécessairement au délai de prescription de l'assignation de l'article 53 de la loi de 1881.

41. Le délit d'usurpation d'identité. Sur le fondement de l'article 226-4-1 du Code pénal, le délit d'usurpation d'identité consiste à : « usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende ». Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. C'est la loi n° 2011-267 du 14 mars 2011 [LOPPSI II] qui a instauré ce nouveau délit réprimant l'usurpation d'identité numérique commise en vue de troubler la tranquillité d'autrui, ou de porter atteinte à son honneur ou à sa considération.
La principale question était de savoir si ce texte pouvait s'appliquer aux personnes morales, ou si dans notre cas seul les chefs d'entreprises, personnes physiques pouvaient s'en prévaloir. Situé dans le Titre II du Code pénal, consacré aux atteintes à la personne humaine, nous devions en déduire une application stricte regrettable. En effet, elles sont les premières victimes de ce type de comportement délictueux. Toutefois et après une recherche dans les travaux parlementaires du 11 février 2010, nous pouvons affirmer que : « dans le silence de la loi, les dispositions (...) s'appliquent aussi bien aux personnes morales qu'aux personnes physiques ».

L'exposition médiatique des entreprises les rend vulnérables à ce type de comportements malveillants : création de faux comptes Facebook ou Twitter, propos désobligeants, ou encore la

89 CA Lyon, 8e ch., 29 janv. 2013, n° 11/05620, SARL Aphysio c/ SARL Avipur 3D. Sur cette décision v. J. LARRIEU, Du passé faisons table rase..., Propriété industrielle novembre 2013, comm. 84.
90 J. LARRIEU, Du passé faisons table rase..., préc.
91 J. LARRIEU, Du passé faisons table rase..., préc.

pratique de l' hameçonnage ou *phishing* (parfois appelé filoutage). Il s'agit d'une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance, afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. Elle se fait le plus souvent par sollicitations de mail.

42. La sanction pénale issue du droit de la consommation. L'entreprise peut également être tentée d'intervenir sur les nombreux sites ou forums dédiés aux avis de consommateurs. Il s'agit d'une stratégie de communication quelque peu agressive. Les pratiques les plus courantes sont :

- L'utilisation de « faux avis » ou « fake review » : consiste à publier de faux avis ou à s'attribuer une communauté artificielle de fans ou d'amateurs, d'une marque, d'un produit ou d'un service. Ces avis sont faux soit parce que le contenu de l'avis est faux, soit parce que l'identité de celui qui le formule est fausse.
- La suppression des avis et commentaires des internautes.

Sanctionnées par le Code de la consommation, les atteintes reçoivent alors les qualifications de pratiques commerciales déloyales à l'article L. 120-1, de trompeuses par l'article L. 121-1 ou encore des pratiques commerciales agressives sur le fondement de l'article L. 122-11. Elles impliquent la double démonstration que d'une part, l'information soit mise à disposition par un professionnel à destination d'un consommateur et que d'autre part, l'information soit en relation avec un produit ou un service. La sanction est alors pénale ou civile, si elle est fondée sur le droit commun de la responsabilité. L'article L. 121-3 du Code de la consommation permet également au juge d'ordonner la cessation des pratiques litigieuses.

En 2011, Frédéric Lefebvre, alors Secrétaire d'État à la consommation a engagé après des contrôles par la DGCCRF cinq procédures contentieuses devant le Tribunal correctionnel à l'encontre de site Internet pour lutter contre les faux avis. Ont notamment été dénoncées les pratiques d'un site de ventes aux enchères de voyages dont les avis de gagnants étaient intégralement faux et rédigés par lui ou encore d'un site de comparateur dans le domaine du tourisme, qui a recruté massivement des stagiaires en charge de publier de faux avis. La DGCCRF a publié le 22 juillet 2014 le rapport des investigations des années 2010-2013 sur les infractions en matière d'avis de consommateurs. Le taux d'anomalies en augmentation avoisine les 45 %, tous secteurs confondus, pour l'année 2013[92].

Depuis juillet 2013, il existe une norme NF Z74-501 relative au traitement des avis de consommateurs en ligne. Publiée par l'AFNOR, elle a pour objectif de fiabiliser le traitement des avis de consommateurs sur Internet. Or, à la suite de la publication de la norme, des gestionnaires de sites internet se sont auto-déclarés conformes à cette norme alors que les pratiques des entreprises n'étaient pas conformes à cette norme. Il s'agit d'une pratique commerciale trompeuse. En juin 2014, l'Organisation Internationale de Normalisation (ISO) a créé créer un comité technique (TC290) pour réunir tous les pays intéressés par les enjeux de l'e-réputation et

92 Source : http://www.economie.gouv.fr/dgccrf/consommation/conso-par-secteur/e-commerce/faux-avis-consommateurs-sur-internet

plus précisément sur le traitement des avis en ligne de consommateurs, sur la base de la norme française publiée en 2013[93]. L'AFNOR assure le secrétariat du nouveau comité technique international.

B- Les sanctions offertes aux personnes morales pour la protection de leurs informations

43. De l'action à la sanction : l'équivalence des effets ? Lorsqu'une personne morale subit une atteinte à ses informations personnelles ou commerciales, elle est susceptible d'engager plusieurs recours fondés, comme nous venons de l'évoquer, tant sur les droits fondamentaux, que sur le droit de la responsabilité ou le droit pénal. Les sanctions varient en fonction de l'action menée et sont classiquement des amendes ou l'octroi de dommages-intérêts. Internet modifie toutefois le rapport à la sanction. En effet, il est parfois moins recherché la punition du droit pénal ou l'indemnisation du droit de la responsabilité, que la restauration d'une bonne image de l'entreprise. Seront alors préférées les sanctions qui ordonnent le retrait du contenu litigieux. Ainsi, lorsqu'un contenu illicite est publié en ligne, le juge peut ordonner sa suppression : demande de suppression auprès de l'auteur des propos ou de l'éditeur du site, demande de suppression auprès de l'hébergeur du site, requête judiciaire à fins de suppression ou encore demande en référé. Ce dernier est organisé aux termes de l'article 6-I-8 de la loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique (LCEN) par une action en référé . Il permet d'ordonner le retrait immédiat des propos litigieux mis en ligne « l'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 ou, à défaut, à toute personne mentionnée au 1, 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 ». Sur ce même fondement, le retrait du contenu litigieux peut également être ordonné par le juge sur requête, hors de toute procédure d'urgence.

Le retrait et la suppression de l'information attentatoire aux intérêts des personnes morales sont souvent indispensables. Elles sont ainsi dotées d'un outil proche de ceux accordés aux personnes physiques pour organiser l'effacement, voire l'oubli. Mais constitue-t-il le but ultime de l'action menée par l'entreprise victime d'atteinte à ses informations commerciales ou personnelles ? Voir effacer – écraser – le contenu en ligne suffit-il à apaiser les bourdonnements générés autour de l'affaire ? Parfois, la publication en ligne de la décision de justice devient le moyen le plus efficace pour restaurer l'entreprise dans la légitimité de ses droits et réparer les atteintes causées à son image[94]. Si la pratique est courante pour signifier des actes reconnus de contrefaçon dans un

---

93Http://www.iso.org/iso/fr/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=5166853.

94 Véritable liberté publique, elle est fondée sur les garanties fondamentales accordées à tout justiciable par d'une part l'article 6 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales telle qu'amendée par le Protocole n°11 entré en vigueur le 1er novembre 1998. D'autre part, le Code de procédure civile dispose à l'article 451 que « Les décisions contentieuses sont prononcées publiquement et les décisions gracieuses hors la présence du public, le tout sous réserve des dispositions particulières à certaines matières ». Enfin, l'article 11-3 de la loi n° 72-626 en date du 5 juillet 1972 (loi n°72-626 du 05 juillet 1972 instituant un juge de l'exécution et relative à la

monde concurrentiel, elle tend à se généraliser pour les autres actions. Or, cette dernière sanction qui correspond il nous semble parfaitement à la gestion actuelle des entreprises de leurs informations, de leur image et de leur réputation est aux antipodes d'un éventuel droit à l'oubli.

réforme de la procédure civile) dispose que « les tiers sont en droit de se faire délivrer copie des jugements prononcés publiquement ».

CHAPITRE 3

Un droit à l'oubli dans le champ des documents administratifs ?[1]

1. L'appel en faveur du droit à l'oubli par une partie des citoyens, relayé par la presse, est aujourd'hui indéniable et révèle une inquiétude lancinante au regard de certains risques impliqués par le développement des nouvelles technologies. « Ordinateurs et Internet offrent à la mémoire des moyens techniques totalement nouveaux »[2], faisant craindre l'établissement d'une société digne des meilleures utopies dans laquelle les individus se trouveraient fichés à vie, confrontés systématiquement aux fautes de leur passé, dénués de toute vie privée et de liberté. Pas de bonheur[3], pas de liberté sans oubli : tel semble être le nouveau credo de nos sociétés technologiques.

2. S'il est le plus souvent évoqué dans le champ de l'Internet[4], le droit à l'oubli présente en réalité un enjeu bien plus vaste. Sa naissance est conditionnée à l'enregistrement ou à la publicité d'une information intéressant son titulaire[5] : pour avoir un intérêt légitime à être oublié, il convient, au préalable, d'avoir été connu. Les documents administratifs interrogent pleinement ce droit dans la mesure où, d'une part, leur création repose sur un processus de consignation d'informations relatives à des personnes physiques dans un support, écrit ou autre. Ils confèrent, d'autre part, une certaine publicité à ces informations, mises à la disposition des différents services compétents. Ces documents sont en effet ceux « produits ou reçus, dans le cadre de leur mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission »[6]. Il peut s'agir notamment de dossiers, de procès-verbaux, de directives, de correspondances, d'avis ou de décisions sous forme écrite,

---

1 par Julie Arroyo, Attachée temporaire d'enseignement et de recherche à la Faculté de droit de Grenoble

2 TRUCHET (D), « À propos du droit à l'oubli et du devoir de mémoire », Mélanges en l'honneur du Doyen Gérard Cohen Jonathan, libertés, justice, tolérance, Bruylant, 2004, vol. II, p. 599.

3 NIETZSCHE (F), La généalogie de la morale, deuxième dissertation, Œuvres, éd J. Lacoste et J. Le Rider, 1993, vol. 1, p. 103.

4 FAVREAU (A), « La délibération de la CNIL du 12 juillet 2011 : une pierre dans l'édifice du droit à l'oubli », Revue Lamy Droit civil, 2012, n° 92, pp. 53-55 ; MARAIS (A), « Le droit à l'oubli numérique », La communication numérique, un droit, des droits, éd. Panthéon-Assas, 2012, pp. 63-84.

5 SÉNAC (C-É), « Le droit à l'oubli en droit public », RDP, 2012, p. 1159.

6 Article 1er de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal. Le Conseil d'État, le 17 avril 2013, a précisé que « s'agissant des documents détenus par un organisme privé chargé d'une mission de service public qui exerce également une activité privée, seuls ceux qui présentent un lien suffisamment direct avec sa mission de service public peuvent être regardés comme des documents administratifs ». CE, 17 avril 2013, n° 342372, La Poste c/ Bigi, mentionné aux tables Lebon.

numérique, informatique ou encore sous forme d'enregistrement sonore ou visuel se rattachant à une activité de l'administration[7]. Ce premier niveau d'enregistrement et de divulgation de l'information au sein des services administratifs permet une réflexion fertile sur le droit à l'oubli. Son existence et son effectivité dépendent du sort réservé par la suite à ces documents, à savoir de leur destruction ou au contraire de leur conservation, de leur éventuelle communication aux tiers, de leur réutilisation, publication, etc.

3. La matière des documents administratifs interroge d'autant plus le droit à l'oubli que les organismes chargés de services publics sont amenés à recueillir une quantité considérable d'informations sur les personnes physiques, au contenu plus ou moins sensible. M. Delmas explique que le développement de l'État providence en France l'a conduit à intervenir « de toutes sortes de façons et, plus qu'ailleurs, dans la vie des gens » et que, de ce fait, les documents administratifs sont « d'abord des documents qui concernent les individus, leurs vies et leurs familles »[8] ; « [c]es papiers ne sont pas des papiers, mais des vies d'hommes »[9]. L'intrusion des nouvelles technologies dans l'administration renforce au demeurant le risque d'atteinte à l'oubli. Les techniques de l'information et de la communication se développent et, avec eux, les procédés de mise en ligne d'informations détenues par l'administration[10]. Les capacités de mémoire se renforcent également au travers, par exemple, de l'archivage électronique[11].

4. Si les effets du droit à l'oubli ne sont pas connus avec certitude en l'absence de consécration explicite par les textes, il semble que les principes régissant le droit public soient de nature à les contredire. Comme l'affirme M. Sénac, « [d]es institutions classiques, telles que l'intangibilité de l'ouvrage public, l'imprescriptibilité des poursuites disciplinaires, l'imprescriptibilité des archives publiques ou les commémorations nationales sont, entre autres, autant d'indices de la difficile acclimatation de l'oubli à l'environnement du droit public »[12]. Le droit des documents administratifs n'échappe pas à cette suspicion puisqu'il connaît une tendance indéniable à l'accroissement de la transparence[13]. Transformée en véritable « maison de verre »[14], l'administration ne semble pouvoir que difficilement s'ériger en débitrice de l'éventuel droit à l'oubli des administrés. Ce constat est d'autant plus problématique que, par ailleurs, le devoir de

---

7 Ne relèvent pas de cette catégorie les documents émanant d'une personne publique procédant d'une activité législative ou judiciaire. VINCENT (J-Y), « Accès aux documents administratifs. - Régime général. Loi du 17 juillet 1978 », JurisClasseur administratif, Fasc. 109-10, 2010, n° 33.

8 DELMAS (B), « Une nouvelle loi sur les archives : "des archives plus riches et plus ouvertes ?" », La revue administrative, 2008, n° 361, p. 374.

9 DELMAS (B), « Une nouvelle loi sur les archives : "des archives plus riches et plus ouvertes ?" », op. cit., p. 378.

10 Sur le processus de numérisation des archives publiques : DOUILLARD (J), « La communicabilité des archives départementales aux sociétés privées : entre orthodoxie et éthiques législatives », JCP A, 2010, n° 35, actu. 608.

11 DE BOISDEFFRE (M), « Administration et archives aujourd'hui », RFAP, 2002, n° 102, pp. 281 et s.

12 SÉNAC (C-É), « Le droit à l'oubli en droit public », op. cit., p. 1156.

13 Avec toutefois quelques limites cf. infra, particulièrement note de bas de page n° 119.

14 Expression utilisée par le Professeur Chevallier : CHEVALLIER (J), « La transformation de la relation administrative : mythe ou réalité ? (à propos de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations) », Dalloz, 2000, p. 580.

mémoire[15] et les nécessités de l'action administrative ont conduit depuis longtemps l'État à organiser la conservation d'archives publiques réputées imprescriptibles, cette « mise en mémoire » aboutissant à la « survie » d'informations relatives aux individus et à leur passé. Ces archives se définissent comme « l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité » de service public[16]. En dépit de l'apparente similitude des deux définitions, les documents administratifs et les archives publiques ne se confondent pas entièrement : si les premiers sont des archives publiques potentielles, toutes les archives publiques ne sont pas des documents administratifs[17]. Celles-ci regroupent, de surcroît, les actes judiciaires ou d'état civil[18] ainsi que les minutes et les répertoires des notaires[19]. Par souci de facilité, l'expression « documents administratifs » sera toutefois employée le plus souvent pour désigner ces documents *stricto sensu* ainsi que les archives publiques.

5. Malgré le fait qu'elles soient guidées par des principes contrariant l'oubli individuel, les normes encadrant les documents administratifs ne demeurent pas indifférentes à la revendication grandissante en faveur du droit à l'oubli, et ce, compte tenu des intérêts primordiaux auxquels cette prérogative satisfait. Elle répond, d'une part, à l'intérêt personnel des titulaires et, plus précisément, à la satisfaction de leur liberté[20]. Celle-ci impliquant la faculté de faire les choix relatifs à sa propre destinée, ce droit concourt à sa réalisation dans la mesure où il permet à ses bénéficiaires de ne pas se trouver systématiquement confrontés à leurs anciennes décisions et, éventuellement, à leurs erreurs[21]. Il leur offre la possibilité de maintenir « ouvert leur avenir »[22] en obtenant « le silence définitif sur [...] [leur] passé »[23]. Cette prérogative contribue, d'autre part, à la satisfaction de l'intérêt général. Selon le Professeur Letteron, la plus ancienne de ses fonctions réside dans la protection de l'État[24], l'organisation de l'oubli des individus permettant de « garantir la cohésion sociale et la paix civile »[25]. Le Professeur Truchet soutient quant à lui que la sécurité juridique implique de laisser au temps faire œuvre d'apaisement en effaçant « de la mémoire du droit positif

15 Sur la contradiction existante entre le devoir de mémoire et le droit à l'oubli : TRUCHET (D), « À propos du droit à l'oubli et du devoir de mémoire », op. cit., p. 1597.

16 Articles L. 211-1 et L. 211- 4 du Code du patrimoine.

17 GOUNIN (Y) et LALUQUE (L), « La réforme du droit d'accès aux documents administratifs », AJDA, 2000, p. 489.

18 Le Conseil d'État a refusé aux actes d'état civil la qualité de documents administratifs : CE, 9 février 1983, n° 35292, Bertin, Lebon, p. 53, AJDA, 1983, p. 402, chron. LASSERRE (B) et DELARUE (J-M). Sur la qualité d'archives publiques des actes d'état civil : article L. 212-1 du Code du patrimoine ; VINCENT (J-Y), « Accès aux documents administratifs. - Régime général. Loi du 17 juillet 1978 », op. cit., n° 99.

19 EVEN (P), « Une nouvelle loi pour les archives », La revue administrative, 2009, n° 367, p. 233.

20 LETTERON (R), « Le droit à l'oubli », RDP, 1996, pp. 389 et s. ; PETIT (F), « La mémoire en droit privé », RRJ, 1997, n° 1, p. 19 ; TRUCHET (D), « À propos du droit à l'oubli et du devoir de mémoire », op. cit., pp. 1596 et s.

21 TRUCHET (D), « À propos du droit à l'oubli et du devoir de mémoire », op. cit., p. 1596.

22 Ibid.

23 LETTERON (R), « Le droit à l'oubli », op. cit., p. 390.

24 LETTERON (R), « Le droit à l'oubli », op. cit., p. 389.

25 LETTERON (R), « Le droit à l'oubli », op. cit., spéc. p. 389 et p. 422. Également : « l'oubli est nécessaire à la vie en commun ». PETIT (F), « La mémoire en droit privé », op. cit., p. 19.

[certaines] circonstances », sous peine de « provoquer des troubles de l'ordre social ou des injustices »[26].

6. Le droit administratif, traditionnellement conçu comme un droit objectif défendant l'intérêt général[27] et imposant l'assujettissement des administrés à la puissance publique[28], ne peut rester insensible à la seconde justification du droit à l'oubli, en lien avec le bien commun. Il n'apparaît pas non plus indifférent au premier fondement de cette prérogative, centré sur la liberté de ses titulaires. En effet, la vision caricaturale du droit du service public ou de la puissance publique l'appréhendant comme un droit exclusivement objectif[29] ignorant totalement les individus et leurs besoins[30] a fait long feu. Les libertés de l'individu sont depuis longtemps protégées par la matière[31] et cette dernière n'apparaît pas hermétique au mouvement, plus général, de subjectivisation du droit dans lequel s'inscrit l'appel en faveur du droit à l'oubli[32]. Ces différentes caractéristiques du droit administratif, à la fois droit d'exorbitance et de sujétion au service de l'intérêt général, et à la fois droit défenseur des prérogatives et libertés de l'individu[33], expliquent que les traces d'une protection de l'oubli puissent être décelées dans le régime juridique applicable aux documents administratifs (2), et ce, malgré l'existence de principes attentatoires à l'oubli de l'individu régissant le droit de ces documents (1).

Section 1- Les principes régissant le droit des documents administratifs attentatoires à l'oubli de l'individu

7. Le champ des documents administratifs apparaît comme une « terre » hostile à l'oubli des administrés. Non seulement ces documents peuvent être conservés en archives publiques (I), mais, en outre, le principe de transparence innerve le droit qui leur est appliqué (II).

---

26 TRUCHET (D), « À propos du droit à l'oubli et du devoir de mémoire », op. cit., p. 1597.

27 BAILLEUL (D), « Le droit administratif en question : de l'intérêt général à l'intérêt économique général ? », JCP A, 2005, n° 13, 1147 ; DELVOLVÉ (P), « Propos introductifs. Droits publics subjectifs des administrés et subjectivisation du droit administratif », Les droits publics subjectifs des administrés, Travaux de l'AFDA - 4, LexisNexis Litec, Collection Colloques et Débats, 2011, p. 3.

28 L'idée de sujétion de l'administré à la puissance publique est inhérente à l'idéologie de l'intérêt général du droit administratif. CHEVALLIER (J), « Les fondements idéologiques du droit administratif français », Variations autour de l'idéologie de l'intérêt général, CURAPP, PUF, 1979, tome II, pp. 3-57, spéc. p. 55.

29 Le Professeur Seiller évoque « la tournure officiellement objective de notre droit administratif ». SEILLER (B), « Avant propos », Les droits publics subjectifs des administrés, op. cit., p. 1.

30 SZYMCZAK (D), « Le droit européen, source de droits publics subjectifs des administrés ? », Les droits publics subjectifs des administrés, op. cit., p. 53.

31 Par exemple : CE, 19 mai 1933, n° 17413 17 520, Benjamin, Lebon, p. 441.

32 FOULQUIER (N), Les droits publics subjectifs des administrés. Émergence d'un concept en droit administratif français du XIXe siècle au XXe siècle, Dalloz, Nouvelle Bibliothèque de Thèses, 2000, pp. 1 et s., spéc. p. 6. D'ailleurs, la première sollicitation du concept de droits publics subjectifs date des années 1930 : BONNARD (R), « Les droits publics subjectifs des administrés », RDP, 1932, p. 695. Récemment sur ce thème : FOULQUIER (N), op. cit. Également le colloque de l'AFDA de 2010 : Les droits publics subjectifs des administrés, op. cit.

33 Sur ces différents aspects du droit administratif : AUBY (J-B), « La bataille de San Romano - Réflexions sur les évolutions récentes du droit administratif », AJDA, 2001, p. 912-926 ; SALES (E), « Vers l'émergence d'un droit administratif des libertés fondamentales ? », RDP, 2004, pp. 207-241.

I-La conservation des documents administratifs en archives publiques

8. Constituées à partir du XVII[e] siècle avec les pièces émanant de l'État et celles présentant un intérêt public[34], les archives publiques connaissent un encadrement juridique véritable depuis la Révolution française[35]. Elles sont désormais régies par la loi du 3 janvier 1979[36] telle que réformée par la loi du 15 juillet 2008[37]. Protégées par le principe d'imprescriptibilité[38], ces « expressions [...] de la mémoire »[39] heurtent le droit à l'oubli en empêchant la disparition d'informations intéressant les personnes physiques contenues dans les documents[40]. La plupart des auteurs[41] définissent en effet le droit à l'oubli comme étant celui d'obtenir « la disparition »[42], « la suppression »[43], l'« effacement »[44] ou encore la non-conservation[45] d'informations relatives à son titulaire. En outre, la loi du 6 janvier 1978 dite « informatique et libertés »[46] est souvent présentée comme une référence pour sa défense[47] au motif qu'elle interdit la conservation des données à caractère personnel issues d'un traitement informatisé « sous une forme permettant l'identification des personnes concernées pendant une durée qui [...] excède [...] la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »[48].

---

34 FAVIER (J), Les archives, PUF, Que sais-je ?, 5e éd. recorrigée, 1991, pp. 19-20.

35 DUCLERT (V), « République et archive », RFAP, 2002, n° 102, pp. 269-276. Cf. le décret du 7 septembre 1790 créant les Archives nationales et la loi du 7 messidor an II organisant la conservation et l'accès aux archives.

36 Loi n° 79-18 sur les archives.

37 Loi n° 2008-696 relative aux archives.

38 Article L. 212-1 du Code du patrimoine.

39 CHIRAC (J), « Discours », Les Français et leurs archives, actes du colloque au Conseil économique et social du 5 novembre 2001, Fayard, 2002, p. 162. En ce sens également : BRAIBANT (G), Les archives en France, La documentation française, Collection des rapports officiels, 1996, p. 9.

40 LETTERON (R), « Le droit à l'oubli », op. cit., p. 407. Sur la contradiction entre l'article 36 de la loi du 6 janvier 1978 (prévoyant les hypothèses d'archivage public des fichiers informatisés) et l'oubli : MARAIS (A), « Le droit à l'oubli numérique », op. cit., n° 28. D'ailleurs, il est arrivé que le droit à l'oubli soit revendiqué dans un litige portant sur l'enregistrement des débats judiciaires et leur conservation dans les archives audiovisuelles de la justice. La Cour de cassation n'a toutefois pas retenu l'atteinte à celui-ci dans cette hypothèse : Cass. crim., 17 février 2009, n° 09-80.558, Bulletin crim., n° 40.

41 Contra : « le droit à l'oubli n'implique pas la destruction des documents ». LASSERRE (B) LENOIR (N) et STIRN (B), La transparence administrative, PUF, Politique d'aujourd'hui, 1987, p. 219.

42 LETTERON (R), « Le droit à l'oubli », op. cit., p. 386. Également en ce sens : CHEVALLIER (J), « La transformation de la relation administrative : mythe ou réalité ? (...) », op. cit., p. 581.

43 MARAIS (A), « Le droit à l'oubli numérique », op. cit., n° 6.

44 DURANTON (M) et FOEGLE (J-P), « Fichage partout, oubli nulle part ? Le Conseil d'État ouvre un boulevard au fichier "TAJ" », Revue des droits de l'homme, 16 juillet 2014, n° 24 et s., spéc. n° 29.

45 PETIT (F), « La mémoire en droit privé », op. cit., p. 41.

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

47 LEMAIRE (F), « Commentaire de la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations », Gazette Palais, 24 octobre 2000, n° 298, pp. 3-12, spéc. sous I A 2 a ; BRAIBANT (G), op. cit., p. 75 ; LASSERRE (B) LENOIR (N) et STIRN (B), op. cit., p. 219.

48 Article 6 § 5 de la loi. Selon la plupart des auteurs, cette disposition protège le droit à l'oubli : ibid ; PONTHOREAU (M-C), « La directive 95/46 CE 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 », RFDA, 1997, p. 136 ; PETIT (F), « La mémoire en droit privé », op. cit., p. 42, note de bas de page 191 ; SÉNAC (C-É), « Le droit à l'oubli en droit public », op. cit., p. 1159.

9. L'archivage des documents administratifs, s'il contrarie l'oubli individuel, se justifie par divers intérêts[49], comme en atteste la célèbre affirmation de Guy Braibant : « [s]ans archives, pas d'État, pas d'Histoire, pas de République »[50]. Ce processus apparaît, d'abord, consubstantiel à l'action de l'État, garant de l'intérêt général. L'efficacité des administrateurs étant conditionnée à leur connaissance du passé[51], les archives publiques leur permettent de prendre les décisions et de correctement administrer, dans la mesure où elles « *retracent et reflètent la procédure et le contenu de* [...] [leur] *action* »[52]. Elles favorisent, ainsi, la continuité de l'État à travers la continuité de son action[53].

10. Ensuite, et même si ce point apparaît plus délicat à appréhender, il semble que les archives publiques participent à l'existence même de l'État ou, du moins, contribuent à asseoir sa légitimité. M. Legendre explique que l'archivage de documents a pour ambition première la « conservation de preuves ayant trait à la légitimité de ce qui se fait »[54], laissant ainsi supposer que, s'agissant des archives publiques, elles concourent à justifier le pouvoir. Ce pouvoir selon l'auteur est « non seulement le pouvoir d'écrire la légalité authentique [...] [, mais] est aussi le pouvoir de montrer », d'où cette conservation presque ritualisée des documents en lien avec ce dernier[55]. Les archives paraissent ainsi assurer une fonction de représentation de l'État, de son action et de sa puissance, le confortant par là dans sa légitimité et son existence[56].

11. Dans la même veine, l'établissement d'archives publiques facilite la constitution d'une mémoire collective[57], elle-même « ossature » de la Nation[58]. Or selon certains, la Nation, c'est-à-dire cet ensemble de personnes unies autour de valeurs, d'une histoire et d'un projet[59], constitue le « sous-bassement nécessaire » de l'État[60]. Et, même s'il est vrai qu'aujourd'hui la plupart des auteurs distinguent les deux entités[61], le travail de la mémoire dans la constitution de l'État demeure incontestable. L'existence d'une histoire commune facilite en effet l'adhésion au pouvoir issu de cette dernière et renforce, par ce biais, la légitimité de l'État en place. Le Professeur Cartier explique à cet égard que la majorité des préambules des textes constitutionnels établissent une

---

49 L'article L. 211-2 du Code du patrimoine évoque l'intérêt public attaché à cet archivage en précisant que la conservation des documents administratifs répond aux « besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques et privées » ainsi qu'à ceux de « la documentation historique de la recherche ».

50 Guy Braibant cité par M. Duclert. DUCLERT (V), « République et archive », op. cit., p. 269. Le rapport étroit entretenu par les archives publiques et l'histoire s'illustre notamment dans un jugement reconnaissant la qualité d'archives publiques aux archives de la France libre. TGI Paris, 20 novembre 2013, n° 12/06156.

51 BRAIBANT (G), « Le passé et l'avenir de l'administration publique », RFAP, 2002, n° 102, p. 213.

52 DE BOISDEFFRE (M), « Administration et archives aujourd'hui », op. cit., p. 280.

53 LAVAISSIÈRE (J), « Le pouvoir, ses archives et ses secrets », Dalloz, 1984, chron., p. 65.

54 LEGENDRE (P), « Une mémoire fonctionnelle », RFAP, 2002, n° 102, p. 226.

55 Ibid.

56 DUCLERT (V), « République et archive », op. cit., p. 270.

57 CHEVALLIER (J), « L'État-Nation », RDP, 1980, p. 1287.

58 KERVICHE (E), « La Constitution, le chercheur et la mémoire », RDP, 2009, p. 1066. En ce sens également : MONNIER (S), « La réforme du droit des archives. À propos de la loi du 15 juillet 2008 », Droit administratif, 2008, n° 11, p. 21.

59 FAVOREU (L) et a., Droit constitutionnel, Dalloz, Précis droit public science politique, 16e éd., 2014, p. 35, n° 41.

60 CHEVALLIER (J), « L'État-Nation », op. cit., p. 1272.

61 COHENDET (M-A), Droit constitutionnel, Montchrestien, 3e éd., 2006, p. 27.

véritable « genèse, dont la véracité historique est parfois sujette à caution, destinée à asseoir la légitimité de l'ordre politique nouveau »[62]. Dans la mesure où l'histoire et la mémoire communes aux membres d'un même groupe tendent à favoriser sa « cohérence »[63], son unité[64], les archives publiques assurent une fonction d'intégration et, ainsi, facilitent l'action de l'État en renforçant l'adhésion des citoyens à son égard[65].

12. Enfin, les archives publiques sont couramment présentées comme un gage du caractère démocratique d'un État[66]. Préserver les traces de son activité permet aux individus non seulement d'exercer leur liberté en ayant accès à des documents intéressant leurs droits, mais aussi de se livrer à une certaine forme de contrôle du pouvoir[67]. Du reste, les archives rendent possibles les recherches historiques ce qui permet d'éviter la propension, caractéristique des régimes totalitaires, à l'instauration d'une histoire officielle[68]. Elles apparaissent consubstantielles à la liberté de la recherche[69] et constituent un « gage du caractère scientifique des travaux des historiens »[70].

13. Au regard de ces différents intérêts publics auxquels satisfait l'archivage, l'intérêt légitime de l'administré à être oublié apparaît de moindre importance. La conservation des documents administratifs facilite, de surcroît, la réalisation d'intérêts d'ordre privé. En tant que sources de renseignements, les archives publiques participent à l'exercice de la liberté d'information[71], l'individu pouvant être amené à faire des recherches d'ordre historique, intéressant la sphère publique, ou davantage personnelles dans la perspective de se renseigner sur ses origines ou de justifier de ses droits[72].

---

62 CARTIER (E), « Histoire et droit : rivalité ou complémentarité ? », RFD const., 2006, n° 67, p. 524. Également en ce sens : KERVICHE (E), « La Constitution, le chercheur et la mémoire », op. cit., p. 1067.

63 PETIT (F), « La mémoire en droit privé », op. cit., p. 17.

64 CHEVALLIER (J), « L'État-Nation », op. cit., p. 1287.

65 CHIRAC (J), « Discours », op. cit., p. 162 : « [...] les archives constituent un élément intrinsèque de notre identité » ; RÉMOND (R), « Introduction », Les Français et leurs archives, op. cit. p. 24 : elles sont « une invitation à une réflexion sur les rapports entre les archives et la mémoire, entre le passé et l'identité nationale ».

66 DUCLERT (V), « République et archive », op. cit., pp. 271-272 ; MONNIER (S), « La réforme du droit des archives. À propos de la loi du 15 juillet 2008 », op. cit., p. 21 ; DE BOISDEFFRE (M), « Administration et archives aujourd'hui », op. cit., p. 283.

67 LASSERRE (B) LENOIR (N) et STIRN (B), op. cit., p. 253 ; PETITCOLLOT (P), « La mémoire du travail gouvernemental », RFAP, 2002, n° 102, p. 292.

68 KERVICHE (E), « La Constitution, le chercheur et la mémoire », op. cit., pp. 1049 et s. ; CARTIER (E), « Histoire et droit : rivalité ou complémentarité ? », op. cit., pp. 523 et s.

69 Sur cette liberté : Cons. const. Décision n° 94-345 DC du 29 juillet 1994, Loi relative à l'emploi de la langue française ; MONIOLLE (C), « Indépendance et liberté d'expression des enseignants-chercheurs », AJDA, 2001, p. 226.

70 EVEN (P), « Une nouvelle loi pour les archives », op. cit., p. 231.

71 Consacrée notamment à l'article 10 de la Convention européenne des droits de l'homme et à l'article 19 du Pacte international relatif aux droits civils et politiques.

72 Mme Chabin évoque plusieurs « catégories » de lecteurs d'archives : CHABIN (M-A), « La communicabilité des archives : l'information, le document, le dossier », La revue administrative, 1995, n° 283, pp. 418 et s. En ce sens également : DE BOISDEFFRE (M), « Administration et archives aujourd'hui », op. cit., pp. 280 et s. Sur le droit à l'information publique, parfois présenté comme un élément essentiel de la « troisième génération des droits de l'homme » cf. BRAIBANT (G), « Droit d'accès et droit à l'information », Mélanges R. E. Charlier, service public et libertés, éd. de l'Université, 1981, p. 703.

14. Parfois également présentées comme un facteur de sécurité juridique[73], les archives publiques répondent donc à un certain nombre d'intérêts publics qui semblent reléguer au second plan les atteintes qu'elles engendrent, par ailleurs, à l'oubli des administrés. Ces atteintes ne résultent pas uniquement de la conservation des documents administratifs : elles dépendent aussi du degré de leur accessibilité et de leur employabilité avant et après leur archivage[74].

II- Le principe de transparence innervant le droit des documents administratifs

15. Le secret a pendant longtemps guidé le fonctionnement de l'administration dans ses rapports avec les usagers. Le refus d'informer les administrés était alors la règle, le droit d'informer l'exception[75]. Essentiellement au service de la protection de l'administration, dans la mesure où il préservait des regards indiscrets certains processus décisionnels[76], le secret administratif visait également, de façon plus ponctuelle, à protéger les administrés[77]. Garant d'une certaine « opacité individuelle »[78], il contribuait dans cette dimension à l'oubli des individus grâce à la dissimulation d'informations les intéressant aux usagers.

16. Alors que le secret administratif était l'allié, même partiellement « conscient », de l'oubli des individus, la transparence se révèle au contraire son pire ennemi : en dissipant le « brouillard » entourant l'administration, en « déchir[ant] le voile qui la recouvre », en la rendant moins « opaque »[79], la transparence contribue à la connaissance et, ainsi, à la mémorisation[80]. Le fait que le droit à l'oubli soit parfois présenté comme revêtant la forme d'un droit à la confidentialité révèle d'ailleurs cette contradiction[81]. Le mouvement en faveur de la transparence administrative, amorcé lors de la Révolution française à travers la publication des lois et des règlements, l'apparition des premières enquêtes publiques et la motivation des jugements[82], s'est véritablement confirmé dans les années 1970[83]. La levée du secret administratif se concrétise alors dans une série de grandes lois

---

73 TRUCHET (D), « À propos du droit à l'oubli et du devoir de mémoire », op. cit., p. 1597.

74 Le droit à l'oubli n'est pas nécessairement atteint par le seul fait de conserver indéfiniment les documents administratifs en archives publiques, dans la mesure où lorsqu'un certain secret entoure cette conservation les informations qu'ils contiennent ne pourront s'inscrire dans les consciences. En ce sens : « le droit à l'oubli n'implique pas la destruction des documents ». LASSERRE (B) LENOIR (N) et STIRN (B), op. cit., p. 219.

75 LEMASURIER (J), « Vers une démocratie administrative : du refus d'informer au droit d'être informé », RDP, 1980, p. 240.

76 CHEVALLIER (J), « Le mythe de la transparence administrative », Information et transparence administrative, PUF, 1998, p. 243.

77 LASSERRE (B) LENOIR (N) et STIRN (B), op. cit., p. 6.

78 LASSERRE (B) LENOIR (N) et STIRN (B), op. cit., p. 55.

79 CHEVALLIER (J), « La transformation de la relation administrative : mythe ou réalité ? (…) », op. cit., p. 580.

80 Pour un exemple de lien établi entre l'oubli et la publication d'informations : DERIEUX (E), « La notion de "publication" - Les insupportables incertitudes du droit », JCP G, 2010, n° 49, 1195. Pour un exemple d'évocation du droit à l'oubli à propos de la question de la communicabilité des archives : CHABIN (M-A), « La communicabilité des archives : l'information, le document, le dossier », op. cit., p. 415. Pour un exemple de lien établi entre l'oubli et la réutilisation de renseignements : PETIT (F), « La mémoire en droit privé », op. cit., p. 31.

81 Sur le droit à l'oubli prenant l'apparence d'un droit à la confidentialité : SÉNAC (C-É), « Le droit à l'oubli en droit public », op. cit., p. 1158.

82 BRAIBANT (G), « Préface », La transparence administrative, op. cit., p. VII.

83 CHEVALLIER (J), « Le mythe de la transparence administrative », op. cit., p. 251.

reconnaissant un droit à l'information au profit de l'administré, telles que la loi du 16 janvier 1978 consacrant l'accès aux fichiers informatisés, celle du 17 juillet 1978 sur l'accès aux documents administratifs et celle du 3 janvier 1979 sur les archives. Ces législations seront par la suite affermies avec l'adoption de la loi du 12 avril 2000 dont le titre premier est consacré à l'accès aux règles de droit et à la transparence[84].

17. Dans le champ des documents administratifs, le contexte de transparence a conduit à l'affirmation progressive du principe de leur libre communicabilité et de leur libre réutilisation. La loi du 17 juillet 1978 a posé le principe de la liberté de communication des documents[85] et a créé la Commission d'accès aux documents administratifs (CADA), autorité administrative indépendante chargée de veiller à son effectivité[86]. En outre, elle a prévu qu'un certain nombre de pièces feront l'objet d'une publication telles que les directives, instructions, notes, etc.[87] Au niveau des archives publiques, ce mouvement en faveur de la transparence s'est traduit par une réduction de leur délai d'ouverture[88] : la loi du 3 janvier 1979 a d'abord abaissé le délai de droit commun de communication des archives de 50[89] à 30 ans[90], puis ce délai a été supprimé par la loi du 15 juillet 2008 et remplacé par un principe de libre communicabilité[91]. La création d'un droit à la réutilisation des informations publiques, introduit dans la loi du 7 juillet 1978 par une ordonnance du 6 juin 2005[92], apparaît elle aussi, mais dans une moindre mesure[93], comme un moyen de « renforcer la transparence de la vie publique »[94]. Elle offre à toute personne la possibilité de réutiliser les informations figurant dans les documents administratifs communicables « à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus »[95]. Cette tendance à l'accroissement de la transparence n'est pas arrivée à son terme et se nourrit actuellement du mouvement de l'open data, prônant une plus grande ouverture

---

84 Loi n° 2000-321 relative aux droits des citoyens dans leurs relations avec les administrations.

85 Il consacre son titre premier à la liberté d'accès aux documents administratifs. Cf. spécialement son article 2.

86 SINNASSAMY (C), « L'effectivité de la transparence administrative : quelle réussite juridique ? », RRJ, 2007, n° 3, p. 1380.

87 Actuellement l'article 7 de la loi du 17 juillet 1978 telle qu'issue de l'ordonnance n° 2009-448 du 29 avril 2009 dispose que « [f]ont l'objet d'une publication les directives, les instructions, les circulaires, ainsi que les notes et réponses ministérielles qui comportent une interprétation du droit positif ou une description des procédures administratives. Les administrations mentionnées à l'article 1er peuvent en outre rendre publics les autres documents administratifs qu'elles produisent ou reçoivent ».

88 GONOD (P), « La réforme des archives : une occasion manquée », AJDA, 2008, p. 1602.

89 Décret n° 52-219 du 27 février 1952.

90 Article 7 de la loi du 3 janvier 1978 dans sa version initiale.

91 Article 1er de la loi du 15 juillet 2008 codifié à l'article L. 213-1 alinéa 1 du Code du patrimoine.

92 Ordonnance n° 2005-650 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques (transposant la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public).

93 Certains auteurs considèrent que le droit à la réutilisation des documents concerne moins l'enjeu de la transparence que des enjeux économiques : VINCENT (J-Y), « Accès aux documents administratifs. - Régime général. Loi du 17 juillet 1978 », op. cit., n° 7.

94 CONNIL (D), « Réutilisation commerciale d'archives départementales : nouvelle décision, nouvelle étape », note sous CAA Lyon, 4 juillet 2012, n° 11LY02325, AJDA, 2013, p. 303.

95 Article 10 de la loi du 17 juillet 1978 tel que crée par l'ordonnance de 2005 et tel que modifié par l'ordonnance 2009-483 du 29 avril 2009.

des données publiques[96]. Le passage d'une logique de communicabilité des documents administratifs à celle d'une libre diffusion de l'information administrative est notamment envisagé[97].

18. La transparence constitue une condition de réalisation de la démocratie administrative[98]. Sa promotion répond à la crise du système démocratique fondé sur le système représentatif[99]. La légitimité de l'administration apparaît désormais moins fondée sur le principe de séparation des pouvoirs, l'élection[100] et le « mythe » de la représentation reposant sur la concordance des volontés des gouvernés et des gouvernants[101] que sur le pluralisme[102] et le contrôle exercé directement par les citoyens sur le processus politique et administratif[103]. Cette vision renouvelée de la démocratie impose de substituer au modèle administratif classique reposant sur la hiérarchie, le secret et l'assujettissement de l'administré, un modèle d'administration plus ouvert, rééquilibré au profit de l'administré, fondé sur l'information, le dialogue et sa participation[104]. La mise en place de la transparence administrative participe à la réalisation de ces nouvelles exigences démocratiques en assurant l'information des administrés, cette information leur permettant de se livrer à une forme de contrôle du pouvoir[105] ainsi que, dans une certaine mesure, d'y participer[106].

---

96 MARCHAND (J), « L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique », JCP A, 2014, n° 7, 2038, n° 7 et s.

97 MALLET-POUJOL (N), « Le double langage du droit à l'information », Dalloz, 2002, p. 2421, n° 8 ; ROBINEAU-ISRAËL (A) et LASSERRE (B), « Administration électronique et accès à l'information administrative », AJDA, 2003, pp. 1325 et s. L'article 29 du troisième projet de loi de décentralisation portant sur le développement des solidarités territoriales et de la démocratie locale entend obliger les communes de plus de 3500 habitants à offrir leurs données publiques au format électronique à la réutilisation du public par une mise en ligne. Projet accessible en ligne sur le site du Sénat : http://www.senat.fr/leg/pjl12-497.html

98 CHICOT (P-Y), « La démocratie représentative : essai de conceptualisation », La revue administrative, 2011, n° 380, p. 143 ; DONIER (V), « Les droits de l'usager et ceux du citoyen », RFDA, 2008, pp. 13 et s.

99 CHEVALLIER (J), « De l'administration démocratique à la démocratie administrative », RFAP, 2001, n° 137-138, p. 221 ; DAUGERON (B), « La démocratie administrative dans la théorie du droit public : retour sur la naissance d'un concept », RFAP, 2011, n° 137-138, p. 24.

100 Celle-ci a longtemps constitué « la clef de voûte et le critère » de la démocratie. CHEVALLIER (J), « De l'administration démocratique à la démocratie administrative », op. cit., p. 218.

101 « La représentation nationale a beau être nous-mêmes, nos droits doivent parfois être défendus contre elle ». AUBY (J-B), « Droit administratif et démocratie », Droit administratif, 2006, n° 2, p. 7.

102 Ibid. C'est en 1990 que le Conseil constitutionnel a défini le pluralisme comme le fondement de la démocratie. Cons. const. Décision n° 89-271 DC du 11 janvier 1990, Loi relative à la limitation des dépenses électorales et à la clarification du financement des activités politiques, § 12.

103 LECLERC (J-P), « Le rôle de la Commission d'accès aux documents administratifs », RFAP, 2011, n° 137-138, p. 178.

104 BRAIBANT (G), « Le passé et l'avenir de l'administration publique », op. cit., p. 22. L'auteur explique que Jean Rivero évoquait dans ses cours les deux modèles successifs de l'administration : militaire et universitaire.

105 SINNASSAMY (C), « L'effectivité de la transparence administrative : quelle réussite juridique ? », op. cit., p. 1375 ; CHEVALLIER (J), « Le mythe de la transparence administrative », op. cit., p. 255.

106 RANGEON (F), « L'accès à l'information administrative », Information et transparence administrative, op. cit., p. 105 ; « le « savoir » étant souvent synonyme de « pouvoir » : LEMASURIER (J), « Vers une démocratie administrative : du refus d'informer au droit d'être informé », op. cit., p. 1240. La transparence est, ainsi, à l'origine de la création d'un droit à l'information administrative. Cf. sur ce point : RANGEON (F), « L'accès à l'information administrative », op. cit., p. 79 ; MAISL (H), « Une nouvelle liberté publique : la liberté d'accès aux documents

19. Si l'archivage et la transparence contrarient l'oubli individuel en assurant la conservation et la publicité d'une multitude d'informations contenues dans les documents administratifs afin de satisfaire l'intérêt public, le droit administratif ne demeure pas insensible à l'intérêt légitime des personnes à l'organisation de leur oubli : la protection de cet oubli peut être décelée dans les exceptions apportées aux principes généraux guidant la matière.

Section 2- Une protection de l'oubli décelable dans le régime juridique appliqué aux documents administratifs

20. La loi « informatique et libertés » est fréquemment présentée comme un modèle de défense de l'oubli et apparaît, en quelque sorte, comme le « droit commun » de la matière[107]. Elle s'applique à l'ensemble des données à caractère personnel et prévoit non seulement l'interdiction de conserver les fichiers contenant de telles données au-delà d'un certain délai[108], mais également l'interdiction de leur communication aux tiers[109]. Elle encadre, en outre, strictement leur utilisation[110]. La loi de juillet 1978 relative aux documents administratifs ne protège pas avec la même intensité l'oubli des administrés, dans la mesure où elle organise l'archivage de ces documents et défend le principe de la liberté de leur communication et de leur réutilisation. Si ces éléments rendent délicate l'identification d'un véritable « droit à l'oubli » en la matière, le régime juridique des pièces administratives révèle néanmoins une certaine défense de l'oubli individuel. L'oubli des administrés se trouve préservé selon différentes modalités (I). Les informations protégées à ce titre (II) demeurent par contre plus limitées que celles défendues par le droit à l'oubli dans le champ de l'informatique et des libertés.

I- Les modalités de protection de l'oubli dans le champ des documents administratifs

21. L'archivage public empêche de reconnaître l'existence, dans le champ des documents administratifs, d'un quelconque droit absolu à la disparition des informations contenues dans ces pièces[111]. En revanche, l'organisation d'un tri préalable à l'archivage « pour séparer les documents à conserver des documents dépourvus d'utilité administrative ou d'intérêt historique ou scientifique,

---

administratifs », Mélanges R. E. Charlier, op. cit., pp. 831 et s. ; PUYBASSET (M), « Le droit à l'information administrative », AJDA, 2003, p. 1307.

107 Cf. supra, n° 9.

108 Article 6 § 5 de la loi.

109 Article 34 : « [l]e responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

110 Article 36 : « [l]es données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; [...] Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa : - soit avec l'accord exprès de la personne concernée ; - soit avec l'autorisation de la Commission nationale de l'informatique et des libertés ; - soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article ».

111 Cf. supra, n° 9. Selon Mme Marchand, le droit à l'oubli ne saurait être appréhendé comme un « impératif absolu d'effacement des données ». MARCHAND (J), « L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique », op. cit., n° 23.

destinés à l'élimination »[112] peut être envisagée comme une forme de protection de l'oubli des administrés. Ces derniers profitent de la destruction des pièces intéressant leur passé et ne présentant aucun intérêt public.

22. Certes, identifier une modalité de protection de l'oubli individuel dans le tri des pièces avant leur conservation ne relève pas de l'évidence puisque, bien avant qu'émerge la revendication du droit à l'oubli et que son existence soit discutée, ce tri était déjà organisé[113]. Cette sélection constitue depuis l'origine une nécessité pratique, dans la mesure où les administrations n'ont jamais eu les capacités de stockage indispensables à la « mise en mémoire » de l'ensemble des documents. Du reste, ce tri apparaît inhérent au processus d'archivage public : celui-ci ne se justifiant qu'au regard de différents intérêts publics et privés, seules les pièces contribuant à leur satisfaction se trouvent logiquement conservées. En réalité, cette sélection semble pouvoir être envisagée comme une manifestation de la prise en compte de l'intérêt des administrés à leur oubli à compter de la loi du 12 avril 2000 dite DCRA. Véritable « compromis entre le "droit à la mémoire" et le "droit à l'oubli" »[114], cette loi a mis en conformité la législation sur les archives publiques avec la loi « informatique et liberté » en organisant un régime spécifique de tri pour les documents administratifs contenant des informations nominatives collectées dans le cadre de traitements automatisés[115]. Elle a ainsi révélé la prise de conscience, par le législateur, des risques impliqués par l'archivage au regard du droit à l'oubli tel qu'organisé par la loi du 6 janvier 1978. À partir de là, il n'est plus question de « la mémoire à tout va »[116], mais d'une mémoire collective respectueuse des libertés des individus et de leur aspiration légitime à se faire oublier de la société.

23. Malgré tout, il convient de ne pas exagérer l'importance de la protection accordée à l'oubli des administrés. Sa défense ne résulte pas d'une véritable conciliation des intérêts, les intérêts publics attachés à l'archivage étant intégralement préservés[117]. En outre, l'ajout progressif de motifs de conservation des archives, à l'origine limités à l'intérêt administratif et historique du document et aujourd'hui étendus à son utilité administrative, à son intérêt historique et statistique pour les données à caractère personnel issues de traitements informatiques, ne révèle pas une évolution propice à l'oubli de l'individu[118].

24. « [L]e secret, comme l'oubli, fai[san]t échec à la mémoire »[119], l'oubli des administrés se trouve, dans d'autres hypothèses, protégé grâce à l'organisation d'une certaine confidentialité des documents[120]. Il en va ainsi en présence de l'interdiction de la communication des pièces

---

112 Article L. 212-2 du Code du patrimoine.

113 FAVIER (J), op. cit., pp. 4-5.

114 CHEVALLIER (J), « La transformation de la relation administrative : mythe ou réalité ? (...) », op. cit., p. 581.

115 Article 5 de la loi dans sa version initiale. La notion d'information nominative a aujourd'hui disparu.

116 LEGENDRE (P), « Une mémoire fonctionnelle », op. cit., p. 223.

117 La conciliation suppose que chaque intérêt en cause soit restreint dans une certaine mesure afin d'aboutir à un « compris » entre ces derniers : SAINT-JAMES (V), La conciliation des droits de l'homme et des libertés en droit français, PUAM, 1995, spéc. p. 7.

118 Articles L. 212-2 et 3 du Code du patrimoine.

119 PETIT (F), « La mémoire en droit privé », op. cit., p. 31.

120 La protection du secret est grandissante : « avec, d'une part, le développement des technologies de l'information et de la communication, d'autre part, celui des activités économiques des personnes publiques, leur privatisation et

administratives d'usage courant. En même temps que la loi du 17 juillet 1978 posait le principe de leur libre communicabilité, elle l'assortissait d'exceptions en instaurant une liste de documents non communicables afin de protéger l'État, mais aussi les particuliers[121]. Une ordonnance du 6 juin 2005[122] a par la suite fait émerger une nouvelle modalité de protection de l'oubli en permettant à l'administration de procéder à la communication des documents non communicables après occultation ou anonymisation de certaines mentions[123]. Ces techniques sont également sollicitées lorsque la publication[124] et la réutilisation des documents administratifs sont envisagées[125]. Leur développement révèle une ambition de conciliation entre, d'une part, l'intérêt de l'individu à la protection de son oubli et les autres intérêts attachés à la non-diffusion d'une information contenue dans un document administratif et, d'autre part, les intérêts publics et privés attachés à la communication[126]. Comparées à l'interdiction de la communication de certains documents initialement organisée par la loi de juillet 1978, l'anonymisation et l'occultation assurent une plus grande transparence en permettant la communication partielle de pièces globalement non communicables tout en maintenant intact l'oubli des individus concernés[127].

25. Si elles concourent toutes les deux à organiser l'oubli de l'individu en faisant en sorte que certaines informations sur sa personne ne soient pas connues des tiers, les techniques de

---

l'ouverture à la concurrence de la plupart d'entre elles, tend à prédominer, à l'heure actuelle, la préoccupation de protéger davantage la confidentialité de certaines informations, qu'il s'agisse de secrets privés ou de secrets administratifs ». DELAUNAY (B), « Nouvelles limitations à l'accès aux documents administratifs », note sous CE, 17 avril 2013, n° 342372, n° 344924, n° 337194, AJDA, 2013, p. 1921. Mme la Professeure Koubi évoque également une interprétation « limitative » du droit à l'information administrative et du droit à la communication des documents administratifs par le juge. KOUBI (G), « Nuances d'un droit à la communication des documents administratifs », note sous CE, 17 avril 2013, n° 3444924, n° 342372, n° 338649, 24 avril 2013, n° 338649, n° 337982, JCP A, 2013, n° 28, 2207.

121 Article 6 de la loi.

122 Ordonnance n° 2005-650.

123 Article 6 § III de la loi du 17 juillet 1978 : « [l]orsque la demande porte sur un document comportant des mentions qui ne sont pas communicables en application du présent article mais qu'il est possible d'occulter ou de disjoindre, le document est communiqué au demandeur après occultation ou disjonction de ces mentions ». La CADA interprète ces dispositions en distinguant les techniques de l'anonymisation et de l'occultation : http://www.cada.fr/les-secrets-des-personnes-physiques,6234.html.

124 La publication de pièces contenant des données à caractère personnel est en effet subordonnée à un « traitement afin d'occulter ces mentions ou de rendre impossible l'identification des personnes qui y sont nommées ». Article 7 de la loi du 17 juillet 1978.

125 Article 13 de la loi du 17 juillet 1978 : « [l]es informations publiques comportant des données à caractère personnel peuvent faire l'objet d'une réutilisation soit lorsque la personne intéressée y a consenti, soit si l'autorité détentrice est en mesure de les rendre anonymes ou, à défaut d'anonymisation, si une disposition législative ou réglementaire le permet ».

126 La communication partielle des documents administratifs est parfois évoquée en terme de « [c]ompromis entre transparence et secret ». GOUNIN (Y) et LALUQUE (L), « La réforme du droit d'accès aux documents administratifs », op. cit., p. 494.

127 DONIER (V), « Les lois du service public : entre tradition et modernité », RFDA, 2006, p. 1224 : « [c]ette disposition consacre un droit à la communication partielle du document [...]. Le principe de transparence semble ainsi bénéficier d'une effectivité croissante ».

l'occultation et de l'anonymisation se distinguent[128]. Le droit à l'oubli revêt généralement l'apparence du droit à l'anonymisation[129], que ce soit en droit privé[130] ou en droit public[131], et recouvre plus rarement la forme de l'occultation. Celle-ci conduit à la dissimulation de certains renseignements sur les individus sans camouflage de leur nom ou de leur identité tandis que la première maintient l'information relative à la personne, mais rompt le lien l'unissant à elle grâce à la dissimulation de son nom ou de son identité. L'anonymisation est souvent utilisée dans le cadre de demandes à des fins statistiques alors que l'occultation « reste à privilégier dans les cas où [elle] ne prive pas la communication d'intérêt et où aucun recoupement n'est possible »[132]. Lorsque, par contre, l'anonymisation ou l'occultation ne permet pas de protéger la personne, l'interdiction de la communication du document prévaut à nouveau. La CADA a ainsi déjà eu l'occasion de préciser que des copies corrigées d'une épreuve écrite d'un concours administratif étaient communicables aux tiers sous réserve de l'occultation de leurs mentions nominatives, à moins que, compte tenu des caractéristiques du concours et en particulier du nombre limité de candidats et de son caractère localisé, ces occultations ne soient pas en mesure de garantir l'anonymat des auteurs des copies communiquées[133]. Lorsque le document n'est pas communicable, les informations qu'il contient sont également préservées du principe de libre réutilisation[134].

26. L'oubli des administrés en présence de documents administratifs d'usage courant est dès lors préservé par le biais d'une anonymisation ou d'une occultation d'un certain nombre d'informations intéressant le titulaire avant leur publication, communication aux tiers et réutilisation ou, si ces procédés ne sont pas possibles dans les deux dernières situations, par le biais de l'interdiction de la communication et de la réutilisation. Lorsque les pièces sont conservées en archives publiques, l'oubli est protégé sensiblement de la même manière, mais pendant un certain délai uniquement[135]. En effet, l'article 6 § III de la loi du 17 juillet 1978 précise que « [l]es documents administratifs non communicables au sens du présent chapitre deviennent consultables au terme des délais et dans les conditions fixées par [...] [le Code du patrimoine] »[136]. Ce « temps

---

128 Même si, généralement, le terme d'anonymisation est employé pour designer ces deux procédés : CHAMINADE (A), « Accès aux documents administratifs et aux archives publiques. À propos de l'ordonnance du 29 avril 2009 », JCP A, 2009, n° 25, actu. 739 (sous le point 2).

129 LETTERON (R), « Le droit à l'oubli », op. cit., p. 401.

130 FAVREAU (A), « La délibération de la CNIL du 12 juillet 2011 : une pierre dans l'édifice du droit à l'oubli », op. cit., pp. 53-55 ; PETIT (F), « La mémoire en droit privé », op. cit., p. 1.

131 SÉNAC (C-É), « Le droit à l'oubli en droit public », op. cit., p. 1158.

132 http://www.cada.fr/les-secrets-des-personnes-physiques,6234.html

133 Avis, 3 décembre 2009, n° 20094046, accessible en ligne sur le site de la CADA. Cf. également : TA Paris, 16 octobre 2012, n° 1008762 et n° 1102751, Société France examen : refus opposé à la demande d'une société tendant à la communication des résultats du baccalauréat au motif que l'anonymisation des documents ne rendait pas impossible l'identification des personnes concernées.

134 Article 10 a de la loi du 17 juillet 1978.

135 L'article 2 de la loi du 17 juillet 1978 dispose que « [l]e dépôt aux archives publiques des documents administratifs communicables aux termes du présent chapitre ne fait pas obstacle au droit à communication à tout moment desdits documents ». Il reste que la réutilisation et la publication du document demeurent toujours subordonnées à son anonymisation lorsque celui-ci contient des données à caractère personnel. Cf. infra, n° 36.

136 La libre communicabilité de l'archive publique conduit également sa liberté de réutilisation. Cf. article 10 de la loi du 17 juillet 1978 prévoyant qu'un document communicable est librement réutilisable sous réserve d'occultation ou d'anonymisation.

de confidentialité » laissé à la personne favorise son oubli, en faisant en sorte qu'aucun tiers n'ait accès à l'information la concernant ni ne puisse la réutiliser pendant une durée pouvant aller de 50 à 100 ans ou plus.

27. Les délais d'ouverture des archives publiques tendent, une fois encore, à assurer un équilibre entre, d'une part, l'intérêt des personnes à leur oubli, mais également leur droit à la vie privée, ces intérêts incitant à la mise en place de délais d'ouverture importants et, d'autre part, les intérêts publics et privés attachés à l'ouverture des archives qui, quant à eux, impliquent un accès rapide à ces dernières[137]. Les débats parlementaires ayant précédé l'adoption de la loi de juillet 2008 témoignent de la difficulté de cette entreprise de conciliation, l'opportunité de nombreux délais ayant été longtemps discutée[138]. L'ambition de conciliation est clairement révélée lorsque les délais d'ouverture des archives sont potentiellement plus brefs que la durée de vie de la personne puisque, dans ces situations, son intérêt à l'oubli risque de n'être que partiellement satisfait afin que les différents intérêts attachés à l'ouverture des archives se réalisent plus rapidement. La protection de l'oubli se révèle alors temporaire, l'individu profitant simplement d'une période relativement longue au cours de laquelle l'information demeurera à l'abri des regards, période de nature à favoriser et non à garantir son oubli. Il en va notamment ainsi pour les registres de naissance et de mariage de l'état civil, communicables à l'issue d'un délai de soixante-quinze ans à compter de la date de leur élaboration[139]. La conciliation est moins évidente dans certaines hypothèses où le législateur a organisé un oubli permanent de la personne, faisant vraisemblablement primer cette exigence sur les différents intérêts publics et privés attachés à l'ouverture rapide des archives. La garantie de l'oubli présente ici un caractère immuable, en conférant à son bénéficiaire la possibilité de ne pas voir diffuser une information le concernant durant toute son existence. La volonté de protéger les mineurs a par exemple conduit à subordonner l'accès aux archives contenant des documents les concernant relatifs notamment « aux enquêtes réalisées par les services de la police judiciaire » et « aux affaires portées devant les juridictions » à l'expiration d'un délai de cent ans à compter de la date du document ou d'un délai de vingt-cinq ans à compter de la date du décès de l'intéressé si ce dernier délai est plus bref[140].

28. L'existence de dérogations permettant la consultation des documents d'archives publiques avant l'expiration des délais évoqués confirme la prétention conciliatrice du législateur, même dans les hypothèses où les délais d'ouverture des archives dépassent la durée de vie de la personne. L'article L. 213-3 du Code du patrimoine précise en effet que l'administration chargée

---

137 DELMAS (B), « Une nouvelle loi sur les archives : "des archives plus riches et plus ouvertes ?" », op. cit., p. 374. Contra : TRUCHET (D), « À propos du droit à l'oubli et du devoir de mémoire », op. cit., p. 1597. Le Professeur Truchet considère que le régime des archives publiques n'organise aucune conciliation.

138 MONNIER (S), « La réforme du droit des archives. À propos de la loi du 15 juillet 2008 », op. cit., p. 24 ; EVEN (P), « Une nouvelle loi pour les archives », op. cit., p. 24.

139 Ou à l'issue d'un délai de vingt-cinq ans à compter de la date de décès de l'intéressé si ce délai est plus court : article L. 213-2 4° e du Code du patrimoine. Également : article L. 213-2 3° du même Code prévoyant la communicabilité de certains documents à l'issue d'un délai de 50 ans, en particulier ceux « qui portent une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable, ou qui font apparaître le comportement d'une personne dans des conditions susceptibles de lui porter préjudice ».

140 Article L. 213-2 5° du Code du patrimoine. Également : article L. 213-2 2° du même Code prévoyant la communicabilité de documents intéressants le secret médical 25 ans après le décès de l'intéressé.

des archives peut accorder une telle autorisation de consultation dès lors que « l'intérêt qui s'attache à la consultation de ces documents ne conduit pas à porter une atteinte excessive aux intérêts que la loi a entendu protéger ». La CADA s'attache « au cas par cas [...] [à] mettre en balance les avantages et les inconvénients d'une communication anticipée, en tenant compte d'une part de l'objet de la demande et, d'autre part, de l'ampleur de l'atteinte aux intérêts protégés par la loi »[141].

29. Ces différentes garanties de l'oubli sont assorties de sanctions, rendant opportune la réflexion sur l'éventuelle existence d'un droit en la matière[142]. La responsabilité administrative peut être engagée pour faire suite à la transmission à des tiers de documents non communicables ou en réponse à leur réutilisation[143]. La saisine du juge administratif n'est alors pas subordonnée à un recours préalable devant la CADA. Un tel recours ne s'impose qu'en cas de refus de communication[144]. Si le document est une archive publique, des sanctions pénales viennent s'ajouter à l'éventuel engagement de la responsabilité administrative. L'article L. 211-3 du Code du patrimoine dispose notamment que « [t]out fonctionnaire ou agent chargé de la collecte ou de la conservation d'archives [...] est tenu au secret professionnel en ce qui concerne tout document qui ne peut être légalement mis à la disposition du public »[145]. Les peines encourues vont, pour l'essentiel, jusqu'à un an d'emprisonnement et 15 000 euros d'amende[146].

30. Si la protection de l'oubli existe dans le champ administratif, elle revêt une dimension plus limitée que celle que connaît le droit à l'oubli dans la loi de janvier 1978. Le champ de la protection confirme ce constat.

II- Les données protégées au titre de l'oubli dans le champ des documents administratifs

31. Alors que le « droit commun » de l'oubli, incarné dans la loi de janvier 1978, concerne l'ensemble des données à caractère personnel, la protection de l'oubli dans le champ des documents administratifs a un objet variable, parfois relatif à l'ensemble de ces données, parfois

---

141 Site de la CADA : http://www.cada.fr/l-acces-aux-archives-par-derogation,6103.html

142 La CADA est par contre incompétente pour sanctionner une méconnaissance du droit à l'oubli, ses pouvoirs de sanction étant limités aux hypothèses dans lesquelles la réutilisation porte sur des données altérées ou dénaturées. Cf. article 18 de la loi du 17 juillet 1978.

143 Pour un exemple d'engagement de la responsabilité d'une commune à la suite de la communication d'un document non communicable : CE, 25 juillet 2008, n° 296505, Mme Eve A. S'agissant de la réutilisation, le juge administratif n'a jusqu'à présent été saisi que de recours dirigés contre des refus de communication aux fins de réutilisation d'informations publiques. Cf. TA de Clermont-Ferrand, 13 juillet 2011, n° 1001584, AJDA, 2012, p. 375, note CONNIL (D) ; CAA Lyon, 4 juillet 2012, n° 11LY02325, AJDA, 2013, p. 301, note CONNIL (D) à propos d'un refus opposé par un département à une demande de communication à des fins de réutilisation commerciale de documents d'archives publiques départementales.

144 CE, sect., 19 février 1982, n° 24215, Mme Commaret, Lebon, p. 78, concl. DONDOUX (P) ; CE, 25 juillet 2008, n° 296505, op. cit.

145 Cf. également article L. 214-3 du Code du patrimoine (même s'il intéresse moins directement les sanctions du droit à l'oubli).

146 Article L. 226-13 du Code pénal.

réduit à certaines d'entre elles seulement[147]. Cet objet contribue d'ailleurs à distinguer l'éventuel droit à l'oubli du droit au respect de la vie privée, préservant quant à lui une sphère d'informations plus restreinte[148].

32. Lorsqu'elle s'incarne dans les exceptions apportées au principe de libre communicabilité des documents administratifs, la défense de l'oubli de l'administré ne porte que sur certaines de leurs données. L'article 6 de la loi de juillet 1978 encadre la communication de ces documents uniquement pour ceux d'entre eux qui, d'une part, intéressent la vie privée et qui, d'autre part, mettent « en cause une personne » selon les termes de la CADA. Cette catégorie recouvre, dans la loi, les documents « portant une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable » et ceux « faisant apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice ». L'oubli alors protégé n'est pas un oubli « neutre » ou « objectif » portant sur toutes les données intéressant l'individu, mais un oubli limité à des données nuisibles, soit se rapportant à son intimité, soit attentant à sa réputation : « oubli-discrétion » et « oubli-apaisement », voire « oubli-rémission », telles sont donc les deux facettes alors présentées par la protection administrative de l'oubli.

33. Au titre de la vie privée, sont protégées les données de l'état civil telles que la date et le lieu de naissance[149], l'âge[150], la situation matrimoniale[151] et plus largement familiale[152]. Les coordonnées personnelles[153] sont également concernées ainsi que la situation financière[154], la formation[155], la situation professionnelle[156], l'appartenance politique ou religieuse[157]. En revanche, le nom et le prénom d'une personne ne font pas, par eux-mêmes, partie des éléments protégés par la vie privée[158]. Demeurent ainsi communicables un document comportant le nom, le grade et l'échelon ainsi que l'ensemble des éléments de rémunération qui ne dépendent pas de la situation

147 Il est vrai que la loi de janvier 1978 confère elle aussi une protection plus importante à certaines données sensibles : cf. article 8 I de la loi.

148 Sur la difficulté de distinguer ces deux prérogatives : LETTERON (R), « Le droit à l'oubli », op. cit., p. 390. Les auteurs se fondent généralement sur le critère tiré du champ du droit à l'oubli, dépassant celui du droit à la vie privée : LETTERON (R), « Le droit à l'oubli », op. cit., p. 413 ; SÉNAC (C-É), « Le droit à l'oubli en droit public », op. cit., p. 1158.

149 Conseil n° 20021461 du 11 avril 2002, accessible en ligne.

150 Avis n° 20062311 du 8 juin 2006, accessible en ligne.

151 Conseil n° 20063240 du 27 juillet 2006, accessible en ligne.

152 Avis n° 20080589 du 7 février 2008, accessible en ligne.

153 L'adresse postale, l'adresse électronique et le numéro de téléphone notamment : conseil n° 20045426 du 16 décembre 2004 et avis n° 20081133 du 20 mars 2008, accessibles en ligne.

154 Le patrimoine immobilier : avis n° 20073900 du 11 octobre 2007. Les revenus perçus : avis n° 20031133 du 13 mars 2003, accessibles en ligne.

155 Par exemple, la formation initiale : avis n° 20071643 du 19 avril 2007. Les diplômes : avis n° 20060579 du 2 février 2006. Le curriculum vitae : avis n° 20074411 du 22 novembre 2007, accessibles en ligne.

156 Les horaires de travail : avis n° 20080612 du 7 février 2008. Les dates de congés payés : conseil n° 20081262 du 20 mars 2008, accessibles en ligne.

157 Un exemple d'avis sur les croyances religieuses : avis n° 20064795 du 9 novembre 2006, accessible en ligne.

158 CE, sect., 30 mars 1990, n° 90237, Mme D., Lebon, p. 85.

familiale ou personnelle des agents ou de leur manière de servir[159], l'arrêté de nomination d'un fonctionnaire[160], les contrats de recrutement de chargés de mission d'un conseil général[161] ou les décisions de nomination et de promotion des agents[162]. Le secret médical interdit pour sa part la communication à la compagnie d'assurance d'un hôpital de rapports élaborés par les médiateurs d'une commission concernant certains patients de l'établissement[163].

34. La seconde catégorie d'informations protégées recouvre, d'une part, les pièces « portant une appréciation ou un jugement de valeur sur une personne physique ». Ces documents sont ceux traduisant « le regard subjectif d'une autorité ou d'un tiers »[164] et renvoient notamment aux notes d'un candidat à un concours[165], aux appréciations d'un jury[166], aux « déclarations d'accident scolaire » consignant un comportement répréhensible d'un élève[167], aux avis d'experts sur un travail scientifique soumis à l'appréciation finale d'une autorité administrative[168] ou encore à la rémunération figurant dans un contrat de travail d'un agent public lorsqu'elle est arrêtée d'un commun accord entre les parties sans référence à des règles la déterminant[169]. En revanche, le classement par ordre de mérite de candidats à un concours est communicable, car il ne porte pas, en lui-même, une appréciation ou un jugement de valeur sur eux[170]. D'autre part, les documents révélant le comportement d'une personne ne sont pas communicables aux tiers uniquement si la divulgation de ce comportement risque de lui être préjudiciable, l'existence de ce risque s'appréciant *in concreto* en fonction du contenu du document et de son contexte[171]. De façon générale, les témoignages et plaintes adressés à l'autorité administrative et dirigés contre une personne ne sont communicables qu'à leur auteur, et non à la personne visée[172]. Est également intransmissible un rapport d'enquête administrative établi à la suite d'un accident mortel, dans la mesure où il contient des éléments d'informations intéressant le comportement de personnes identifiées[173].

35. La longueur des délais d'ouverture des archives publiques, dans lesquels se matérialise la protection de l'oubli, dépend là encore, et entres autres[174], du type d'information protégée,

---

159 Conseil n° 20072196 du 7 juin 2007, accessible en ligne. Également : site de la CADA : http://www.cada.fr/les-secrets-des-personnes-physiques,6234.html ; ROBINEAU-ISRAËL (A), « Administration électronique et accès à l'information administrative », op. cit., p. 1329.

160 Avis n° 20050537 du 3 février 2005, accessible en ligne.

161 Avis n° 19950659 du 16 mars 1995, accessible en ligne.

162 Avis n° 20000261 du 20 janvier 2000, accessible en ligne.

163 Conseil n° 20091710 du 14 mai 2009, accessible en ligne.

164 Selon les termes de la CADA : http://www.cada.fr/les-documents-mettant-en-cause-une-personne,6236.html

165 CE, Ass., 8 avril 1987, n° 45172, Ministre de l'urbanisme et du logement c/Ullmo, Lebon, p. 143.

166 Avis n° 20063366 du 31 août 2006, accessible en ligne.

167 Conseil n° 20091694 du 14 mai 2009, accessible en ligne.

168 Conseil n° 20071946 du 26 juillet 2007, accessible en ligne.

169 CE, 24 avril 2013, n° 343024, Syndicat CFDT Culture, mentionné aux tables Lebon.

170 Avis n° 20091037 du 2 avril 2009, accessible en ligne.

171 http://www.cada.fr/les-documents-mettant-en-cause-une-personne,6236.html

172 Pour les rapports d'inspection au sein d'un service : conseil n° 20080070 du 10 janvier 2008, accessible en ligne.

173 Conseil n° 20054519 du 24 novembre 2005, accessible en ligne.

174 Cette durée d'ouverture est, en outre, fonction des personnes concernées, dans la mesure où une protection particulière est accordée aux mineurs. Cf. supra, n° 27.

autrement dit de sa plus ou moins grande sensibilité. Les informations couvertes par le secret médical sont ainsi communicables à l'issue de délais plus importants que celles portant simplement une appréciation sur un individu[175]. Les archivistes reprennent pour l'essentiel les critères de la CADA afin d'apprécier la communicabilité d'un document. Ils veillent toutefois à ne pas indexer complètement les régimes de communication, l'écoulement du temps pouvant influer sur les informations protégées au titre de la vie privée ou sur celles mettant en cause une personne[176]. Par exemple, un document dont la communication avait été refusée avant son classement en archives publiques au motif qu'il comportait l'adresse personnelle d'un individu nommé n'est pas nécessairement soumis au délai de 50 ans applicable aux pièces portant atteinte à la vie privée, « car l'adresse en question, recherchée dans un contexte contentieux, dans le "feu de l'action", devient trente ans plus tard une information sans conséquence, dans un dossier d'archives, pour un observateur qui n'a aucun lien avec la personne citée »[177].

36. Le droit des documents administratifs tend, dans d'autres hypothèses, à favoriser la disparition du souvenir de toute donnée à caractère personnel. Cette donnée est définie par l'article 2 de loi « informatique et libertés » comme étant l'« 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 »[178]. L'oubli alors protégé est un oubli plus « neutre », plus « objectif » en ce qu'il concerne toutes les informations se rapportant à un individu identifiable, même les plus anodines, qu'elles concernent ou non à sa vie privée, qu'elles lui portent ou non préjudice. Le champ de la protection de l'oubli est ainsi étendu lorsqu'il s'agit d'encadrer la publication et la réutilisation des documents administratifs : aucune publication[179] ou réutilisation[180] ne peut être opérée sans que la totalité des informations portant sur un individu identifiable soit occultée ou anonymisée. Le nom d'une personne est protégé à ce titre, alors que sa communication aux tiers n'est pas nécessairement prohibée, cet élément ne constituant pas une information le mettant en cause ou intéressant sa vie privée[181]. Sont ainsi communicables aux tiers sans anonymisation ni occultation, mais ne peuvent être ni publiés ni réutilisés sans recours préalable à ces techniques, les listes du personnel enseignant faisant simplement apparaître les noms, les disciplines, les échelles de rémunération, les quotités de service et les statuts de ces agents[182], l'organigramme d'une commune[183], les décisions de nomination ou de promotion des

---

175 Article L. 213-2 2° et 3° du Code du patrimoine.

176 Selon Mme Chabin, en matière d'archives le document prime l'information lorsqu'il s'agit d'apprécier sa communicabilité. CHABIN (M-A), « La communicabilité des archives : l'information, le document, le dossier », op. cit., pp. 417 et s.

177 CHABIN (M-A), « La communicabilité des archives : l'information, le document, le dossier », op. cit., p. 421.

178 Pour un résumé de l'évolution dans la loi et la pratique ayant mené de la notion d'information nominative à celle de donnée à caractère personnel : GOUNIN (Y) et LALUQUE (L), « La réforme du droit d'accès aux documents administratifs », op. cit., pp. 487-488.

179 Article 7 de la loi du 17 juillet 1978.

180 Article 13 de la loi du 17 juillet 1978.

181 Cf. supra, n° 33.

182 Avis n° 20073195 du 13 septembre 2007, accessible en ligne.

183 Conseil n° 20060660 du 2 février 2006, accessible en ligne.

agents publics[184], la liste du personnel d'un institut médico-éducatif affilié à une caisse de retraite complémentaire et de prévoyance[185], etc.

37. Partant, il semble que le champ de défense de l'oubli soit fonction du degré de publicité accordée à l'information. En effet, plus le risque d'atteinte à l'oubli est grand, c'est-à-dire plus la publicité conférée à l'information est importante, plus le champ des données protégées est large. Ainsi la publication et la réutilisation des documents administratifs, à même d'atteindre fortement l'oubli de l'intéressé en permettant une large diffusion de l'information, sont systématiquement subordonnées à l'anonymisation ou l'occultation de l'ensemble de leurs données à caractère personnel. À l'inverse, la communication aux tiers des pièces administratives, de nature à attenter moins vigoureusement à l'oubli en limitant la prise de connaissance de l'information aux seules personnes ayant procédé à la demande de communication, est encadrée pour certaines données à caractère personnel uniquement. Un avis de la CADA est révélateur de ce lien de dépendance unissant le champ de protection de l'oubli au degré de publicité conféré au document. Après avoir affirmé le caractère communicable d'un ensemble de rapports de l'inspection générale de la Ville de Paris, elle a pris soin de préciser aux auteurs de la saisine que, s'ils souhaitaient les mettre en ligne sur le site officiel de la commune, « elle recommandait de supprimer l'ensemble des noms propres y figurant »[186]. Selon M[me] Robineau-Israel et M. Lasserre, « ceci fait apparaître la différence fondamentale qui existe entre la communication à une personne, sur sa demande, d'un document papier et la mise à disposition du public, de manière universelle et permanente, du même document sous forme numérique »[187]. Le passage, actuellement envisagé, d'une logique de communicabilité de l'information à celle de sa libre diffusion semble par conséquent imposer une protection accrue de l'oubli individuel, notamment par l'élargissement des données protégées.

38. Il ressort de ces développements que le régime juridique des documents administratifs préserve indéniablement l'oubli des administrés. La protection de cet oubli se matérialise dans la destruction des pièces ne présentant aucun intérêt public à l'issue de leur délai d'usage courant ainsi que dans l'organisation de la confidentialité de certains documents à travers l'interdiction de leur communication ou réutilisation, leur anonymisation ou l'occultation de certaines de leurs données, pendant une durée plus ou moins importante en présence de documents archivés. Résultat d'une conciliation de différents intérêts[188], d'une modulation des attentes individuelles et collectives légitimes en démocratie, la défense de l'oubli se révèle néanmoins plus frileuse que celle organisée par la loi « informatique et libertés ». En effet, la protection, parfois limitée à certaines données à caractère personnel, se matérialise uniquement dans des dérogations apportées aux principes d'archivage et de transparence présidant la matière et connaît, par ailleurs, un certain nombre d'exceptions justifiées par l'intérêt général. Pour ces raisons, la reconnaissance de l'existence d'un

---

184 Avis n° 20000261 du 20 janvier 2000, accessible en ligne.

185 CE, 8 mars 1995, n° 125185, M. Adolphe X Torren, mentionné aux tables Lebon.

186 Conseil n° 20030626 du 6 février 2003, accessible en ligne.

187 ROBINEAU-ISRAËL (A) et LASSERRE (B), « Administration électronique et accès à l'information administrative », op. cit., p. 1328. En ce sens également : DELMAS (B), « Une nouvelle loi sur les archives : "des archives plus riches et plus ouvertes ?" », op. cit., p. 374.

188 La « balance des intérêts » est prônée pour résoudre les conflits entre le droit à l'oubli et les autres intérêts. MARAIS (A), « Le droit à l'oubli numérique », op. cit., n° 30.

véritable « droit à l'oubli » dans le champ des documents administratifs demeure, à ce jour, discutable.

TROISIEME PARTIE

Le droit à l'oubli, approches comparatives

CHAPITRE 1

Sens et possibilité d'un droit à l'oubli en droit anglais[1]

Section 1- Prolegomenes[2]

I- L'idée d'un droit à l'oubli

1. La question de l'émergence prospective d'un *droit à l'oubli* n'a pas surgi d'une spéculation théorique, mais bien au contraire de la constatation empirique de l'existence d'un sérieux problème[3]. Ce problème est apparu avec l'affaire dite du *Docteur Feldmar*, et celle dite du *Pirate ivre*. Dans la première affaire, le docteur Andrew Feldmar, un psychothérapeute canadien s'était vu refuser l'accès au territoire des Etats-Unis, à son arrivée à l'aéroport. L'agent des douanes avait tapé son nom sur *Google*, avant de tomber sur un article écrit par Feldmar dans les années 70, dans lequel il expliquait avoir expérimenté sur lui-même du LSD. Au moment de la parution, le LSD venait à peine d'être classé sur la liste I des produits stupéfiants, et de nombreuses expérimentations avaient eu lieu à une époque antérieure, dans un cadre légal et médical. L'information était remontée sur *Google*, car le Docteur Feldmar fait partie des praticiens favorables à l'utilisation médicale de l'acide lysergique diéthylamide (LSD 25), notamment pour soigner l'alcoolisme par une prise unique[4].

---

1 par François Viangalli, Maître de conférences à la faculté de droit de Grenoble

2 L'auteur tient à remercier l'université d'oxford et en particulier david erdos, aujourd'hui lecturer in law and the open society and fellow of trinity hall à l'université de cambridge, pour son aide précieuse dans l'étude in situ des arcanes de la jurisprudence anglaise.

3 la question a déjà fait l'objet de travaux approfondis. V. Ainsi, ex multis : v. Mayer-schönberger, delete, the virtue of forgetting in the digital age, princeton university press, 2009d. Solove, daniel j. Solove understanding privacy, harvard university press, 2008; richard clayton & hugh tomlinson, privacy and freedom of expression, oup, 2010; giusella finocchiaro, la memoria della rete e il diritto all'oblio, il diritto dell'informazione e dell' informatica, 2010-2, p. 391; steven c. Bennett, the right to be forgotten:reconciling and us perspectives, berkeley journal of international law 2012-161; g. Wei, effectively protecting private facts privacy and confidentiality, 2012, 24 sacl. V. Aussi the 'right to be forgotten' and beyond: data protection and freedom of expression in the age of web 2.0, séminaire organisé à l'université d'oxford le 12 juin 2012. Les transcriptions peuvent être consultées à : (www.csls.ox.ac.uk/conferences/oxpilsconference2012/report.php).

4 Dans un cadre médical, la morphine est ainsi utilisée en France pour son effet antalgique. Au Canada et au Royaume-Uni, les hôpitaux utilisent si nécessaire un dérivé plus puissant, la diacétylmorphine, c'est-à-dire ni plus, ni moins que ce que l'on appelle dans la rue l'héroïne. Mais il s'agit bien évidemment d'un usage médical et non récréatif, ce qui évidemment n'a strictement rien à voir avec la toxicomanie. Accuser rétrospectivement le Docteur Feldmar d'avoir été un toxicomane relevait de la même façon, de l'ignorance historique et scientifique la plus complète. Mais encore faut-il avoir des notions scientifiques en la matière, ce que Google ne fournit pas sur sa page de résultats. D'où le problème...

Dans la seconde affaire, une étudiante, *Stacy Snyder*, travaillant dans un établissement d'enseignement secondaire et aspirant à y être recrutée, avait publié sur le net une photographie d'elle-même déguisée en pirate et tenant à la main une bouteille d'alcool. La photo avait circulé, et la personne n'avait pu réussir à l'effacer complètement. Elle était remontée jusqu'à la direction, laquelle avait finalement décidé de ne pas le recruter. S. Snyder fut ainsi une des premières victimes de l'indélébilité du web.

2. Ces deux cas ont fait apparaître à Viktor Mayer-Schönberger, de l'Université d'Oxford, la nécessité de réfléchir sur l'opportunité d'introduire un oubli numérique de l'information. La raison à cette nécessité réside en effet dans la différence fondamentale de la mémoire humaine et de la mémoire virtuelle.

3. La mémoire humaine ne fonctionne pas, en ce qui la concerne, comme le vulgaire l'entend. Elle ne constitue pas une sorte de réservoir dans lequel l'esprit vient puiser à volonté des informations archivées, à la manière d'une banque des souvenirs. En réalité, on sait aujourd'hui que le processus de la mémoire repose bien au contraire sur la sélection des informations et l'*effacement* des données non pertinentes. Il y a déjà un siècle, Freud avait étudié l'aphasie et découvert que les aphasiques sont précisément des individus chez qui le processus d'effacement s'est arrêté, de sorte que leur esprit, et notamment l'expression langagière, située dans les aires de Broca et de Wernicke, est bloquée à leur dernière intervention en date. Soigner un aphasique, c'est donc rétablir l'effacement pour pouvoir « relancer la machine » et leur permettre de recommencer à interagir avec leur environnement en oubliant[5].

4. La mémoire virtuelle, quant à elle, fonctionne exactement d'une façon opposée. Que l'on entende cette mémoire comme l'enregistrement d'une trace, le dépôt d'une information dans une base d'archive, la hiérarchisation de l'information ou la continuité des données les plus récurrentes, un première caractéristique fondamentale demeure : le web ignore le temps[6]. De la même façon, la mémoire numérique est potentiellement illimitée.Le nombre d'informations étant gigantesque, la mémoire numérique écrase en étendue la mémoire humaine. La mémoire cérébrale est à la mémoire du web ce qu'un grain de sable est au Sahara tout entier[7]. Par ailleurs, à la différence de la mémoire humaine, la mémoire numérique se compose d'une immense extension d'informations égales et *non contextualisées*. En effet, lorsque l'agent des douanes a consulté la page de *Google* sur le docteur Feldmar, il en a tiré une information objective, la consommation d'une substance *à ce jour* illicite. Mais cette page n'a pas recontextualisé le sens de cette information. Bien sûr, on aurait pu attendre de l'agent des douanes qu'il opère cette contextualisation lui-même, mais il semble bien, comme le sketch de Fernand Raynaud l'avait dit en son temps, qu'une telle attente fût inespérée… Pour le dire autrement, le *Page Rank* ne préjuge pas de la qualité ni du sens réel de l'information. Pour filer la métaphore, une information

---

5 V.D. Greenberg, Freud and his Aphasia Book : Language and the Sources of Psychoanalysis, Cornell University Press, 1998; et pour l'étude originale de Freud : Contribution à l'étude des aphasies, PUF, 2009

6 G. Finocchiaro, art. préc.

7 Rien qu'en une seule journée, Google manipule une quantité d'information équivalente à 24 petabytes, soit largement plus que la quantité d'information contenue par la Bibliothèque nationale de France dans son ensemble… Sur cette extension des capacités de stockage et de calcul : V. Mayer-Schönberger & K. Kukier, Big Data, Kindle ed, 2013, loc. 134/8426.

décontextualisée équivaut à une ligne abstraite artificiellement d'un livre, au milieu d'une bibliothèque toute entière.

5. Face à cette mémoire virtuelle ainsi entendue, qui peut avoir des conséquences déplaisantes voire déterminantes sur la vie réelle, laquelle ne repose pas quant à elle sur les mêmes processus et les mêmes représentations, l'affirmation d'un *droit à l'oubli*, un *Right To Be Forgotten*, aurait pour fonction d'établir un processus de transition entre le monde virtuel et le monde réel. Il servirait à protéger la personne physique dans son environnement réel, et à lutter contre une forme de mensonge, innocent ou volontaire, par abus de contexte[8].

6. Un tel droit, viendrait-il à être institué, se heurterait cependant à un obstacle technique de taille : sa possible inefficacité pratique. En effet, le web n'oublie pas et il n'est pas techniquement possible d'effacer complètement une information de l'ensemble des serveurs, bases de données et ordinateurs personnels de la planète. A proprement parler, l'information n'est pas effaçable. Il existe même sur le web des sites de récupération des informations, tels que *Way Back Machine* par exemple[9], qui permettent de retrouver l'état antérieur d'un site depuis lors modifié ou supprimé.

7. Un tel obstacle ne doit pas être exagéré. Et ce, pour deux raisons. La première est qu'il est toujours possible, à défaut d'effacer, d'*enfouir* les données. L'enfouissement, à l'instar de son opposé, le référencement, constitue l'une des activités les plus prisées actuellement dans le domaine de l'internet. Gérer sa *réputation numérique* constitue désormais un luxe que s'offrent beaucoup de chefs d'entreprise. Des sociétés spécialisées ont d'ailleurs vu le jour à cette fin. Tel est le cas par exemple de la société *Reputation Squad*, une agence de communication spécialisée dans la réputation digitale[10]. La seconde raison à cela est que l'avenir du web, le futur web 3.0, pourrait bien être celui de la contextualisation des informations. L'émergence d'un web

---

8 Lorsque je dis quelque chose, l'action que je produis résulte non seulement de ce que je signifie intérieurement, mais aussi de la façon dont mon affirmation est comprise par l'auditoire en fonction du contexte, du climat intellectuel du moment, de la sémantique actuellement en usage, voire, parfois, des capacités intellectuelles de l'auditeur.... En ce sens, un grand nombre d'affirmations contiennent, fût-ce à titre incident, un élément performatif, pour reprendre l'expression d'Austin. Sorties de leur contexte, certaines phrases peuvent acquérir un sens complètement différent de celui qu'elles pouvaient avoir initialement pour celui qui les a proférées. Pour rester dans le même domaine que celui de l'affaire Feldmar, un exemple très simple peut ainsi montrer avec quelle facilité il est facile de commettre de tels mensonges par abus de contexte. Imaginons que j'affirme lapidairement que « Freud était un drogué, consommateur compulsif de cocaïne ». La phrase porte une accusation grave sur une figure considérable de la science et de la philosophie du XXème siècle, et le présente sous le jour d'un patient atteint d'une maladie psychiatrique grave, la toxicomanie. Sortie du contexte temporel, culturel et médical de la fin du XIXème siècle, et lue à l'instant présent selon les grilles de lecture de notre société contemporaine, cette accusation est fausse. A l'évidence, Freud n'était pas Christiane F... En revanche, il est exact que Freud a, l'instar d'Emile Zola par exemple, consommé de la cocaïne à l'époque où les effets destructeurs de cette substance n'étaient pas encore connus, où celle-ci était parfaitement légale, quand elle n'était pas tout simplement prescrite sur ordonnance par un médecin. Le re-contextualisation de l'information dans l'environnement d'ignorance scientifique de l'époque redonne par conséquence à l'évidence à cette information anecdotique sur la vie de Freud son véritable sens et fait apparaître l'abus de contexte que la phrase sus-énoncée peut constituer. Elle n'est pas fausse en soi, mais le devient lorsqu'elle acquiert par changement de contexte un pouvoir de sous-entendu tout à différent. V. notamment sur ce point : J.L Chassaing, Freud et la coca, in : J.L. Chassaing, J. Béraud, O. Bézy, P. Claveyrole, Cocaïne, Aphasies : Etudes des textes préanalytiques de Freud, Eres, 2006

9 http://archive.org/web/

10 http://www.reputationsquad.com/

sémantique, qui resituerait chaque information dans un contexte éclairé par des liens intelligents, et non par de simples liens hypertextes, fortuits ou commerciaux, est ainsi prédite par des auteurs comme Tim Berners Lee[11]. Le droit à l'oubli n'est pas une chimère, mais bien une possibilité envisageable.

8. Si l'on envisage l'institution d'un tel droit, il semble approprié de le définir comme le droit d'une personne à empêcher la publication, ou, à tout le moins, le référencement d'une information publiée la première fois dans le passé, après qu'un laps de temps suffisant s'est écoulé depuis cette première publication[12].

9. Ainsi entendu, le droit à l'oubli n'est pas inexistant en droit comparé. En droit italien, par exemple, le tribunal de Rome a pu ainsi interdire à un journal de publier des photographies d'un film licencieux tourné par un acteur célèbre, de nombreuses années en arrière, avant qu'il n'accède à la célébrité[13]. Il ne s'agit donc pas d'une pure invention, ni d'un instrument issu du seul avènement du web 2.0.

10. Les propriétés d'un tel droit sont doubles. En premier lieu, il exerce une fonction de protection contre l'hypertrophie du passé. Le présent s'infère de celui-ci, mais la personne doit construire son avenir, et non revivre en permanence, à l'instar d'un aphasique, une séquence du passé. Le droit à l'oubli protège la personne contre la résurgence et l'anamnèse. Il exerce aussi, en second lieu, une fonction d'objectivation de l'identité personnelle. Celle-ci n'est pas plus définie intérieurement par la personne, mais surtout extérieurement à travers la définition du *profil* numérique de celle-ci. L'individu n'est pas ce qu'il ressent être, mais de façon prépondérante ce que l'on définit de lui par algorithme. Par exemple, l'auteur de ces lignes n'est pas ici en train de réfléchir, il est avant toute chose ce que *Google* dit de lui, et il est fort probable que l'instant présent consacré à la rédaction du présent texte n'y soit pas recensé. Il est donc figé dans l'instant passé, recensé abstraitement par le moteur de recherche, dans une page plus ou moins constante de résultats de recherche, et non concrètement situé dans le temps et l'espace à l'instant présent. Or cette recension agit sur la psychologie de la personne qui se voit sur *Google* d'une façon différente qu'elle ne se voyait jadis dans un miroir. Le web agit non pas comme un miroir physique qui actualise l'image de la personne à chaque instant, mais comme un miroir déformant fabriqué par un programme collectif, qui transforme la vision que la personne a d'elle-même, et s'actualise à un rythme et sur la base de paramètres différents, qui ne dépendent pas de ladite personne.

11. Les fondements, enfin, d'un tel droit sont potentiellement divers. Ainsi, dans la jurisprudence italienne, le droit à l'oubli est fondé sur l'identité personnelle. La re-divulgation nocive d'une information tombée dans l'oubli est considérée, selon l'expression de Scalisi, comme une *lésion de l'identité personnelle*[14]. Rien n'empêche toutefois de considérer que le droit à l'oubli doit être fondé sur le *droit à la réserve* dont disposerait chaque personne à l'égard des autres. En revanche, il ne semble pas opportun, sauf erreur de notre part, de fonder celui-ci sur un *droit à*

---

11 V. sur ce sujet : G. Shroff, The Intelligent Web, Oxford University Press, 2013, p. 150 ; T. Berners-Lee, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web, Harper ed, 2000, p. 157 et svts.

12 G. Finocchiaro, op. cit.

13 Pret. Roma, 10 feb. 1988, Temi rom., 1988, 148 ss, n. C. & F. Acciai

14 G . Finocchiaro, op. cit.

modifier le passé. Le droit à l'oubli n'est ni la machine à explorer le temps de Wells, ni un appareil de propagande destiné à réécrire l'histoire pour l'expurger de tel ou tel fait contraire à la doctrine officielle du moment.

12. Au-delà de ses fondements théoriques, le droit à l'oubli peut être prôné à deux degrés différents. Un premier degré consiste à le concevoir comme un instrument de simple réaction à un abus ponctuel. Il s'agit alors de retenir une conception stricte de l'oubli. Un second degré consisterait à retenir au-delà une conception extensive de l'oubli, pour affirmer un droit à l'autodétermination informationnelle de la personne. L'individu aurait le droit de définir la façon dont il apparaît sur le web, c'est-à-dire en fin de compte de se déguiser, pour ne pas dire se travestir, pour offrir l'image qu'il souhaite. La proposition de Viviane Reding semble aller davantage vers cette conception extensive que vers la version limitée de ce droit, si l'on en juge par ses termes : « *Internet users must have effective control on what they put online and be able to correct, withdraw or delete it at will* ». Les internautes ont ainsi le droit « *to have their data fully removed when it is no longer needed for the purposes of which it was collected*"[15].

13. Quoiqu'il en sera à terme, un tel droit ne peut probablement pas être institué efficacement à l'échelle nationale. En effet, sa mise en œuvre se heurtera nécessairement au principe de liberté de circulation des services énoncé par l'article 56 du TFUE. Le fournisseur de l'information invoquera en effet la législation de son pays d'origine pour contester systématiquement la mise en œuvre du droit en question dans un autre Etat membre que le sien ; ce qui ouvrira la voie à une inflation contentieuse. Il est donc préférable de l'instituer, si besoin est, à l'échelle de l'ordre juridique de l'Union. Mais il faudra alors trouver un accord au Conseil, outre le Parlement bien entendu, et de ce fait trouver un terrain d'entente avec le Royaume Uni, pays très attaché à sa conception de la liberté d'expression, et à son concept accessoire de *Privacy*.

II- La privacy en common law

14. Historiquement, le développement de la Privacy s'est fait concomitamment à l'expansion de la photographie. Alors que l'action en diffamation protège la réputation, la Privacy protège elle les sentiments personnels (personal feelings), comme l'écrivent en 1890 Warren et Brandeis[16]. Il s'agit d'un outil réactif, pas d'un droit à l'autodétermination.

15. Deux conceptions de la Privacy sont envisageables. Une conception essentialiste, tout d'abord, consiste à la percevoir comme une entité existante en soi et dont il importe de défendre l'inviolabilité. A l'inverse, une conception particulariste, revient à l'envisager comme une boîte à outils contenant différentes actions judiciaires (remedies) pouvant offrir une protection réactive appropriée à la personne. Elle est alors une simple thématique regroupant des actions employées dans un cadre factuel comparable, c'est-à-dire un parapluie pour une pluralité de termes (an umbrella for a plurality of terms), selon l'expression de Daniel Solove[17].

16. Quoiqu'il en soit, il est acquis que le terme Privacy présente en Common Law un caractère polysémique. Daniel Solove perçoit par exemple en elle 6 branches :

---

15 http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm

16 The Right to Privacy, 4 Harvard Law Review, 193 (1890)

17 Understanding Privacy, préc.

- un droit à la solitude (*Right To Be Let Alone*)
- un droit à l'accès limité à la personne (*Limited Access to The Shelf*)
- un droit au secret (*Secrecy*)
- un droit au contrôle de l'information personnelle (*Control Over Personal Information*)
- un droit à la protection de la personnalité (*Personality, Individuality & Dignity*)
- un droit à l'intimité (*Intimacy*)[18] .

Mieux encore, Richard Posner, de l'Université de Chicago, y adjoint quant à lui un *droit à la manipulation des informations*, par l'enfouissement de celle-ci, ce qui est très proche d'un droit à l'oubli[19].

17. Les fondements d'un tel droit sont d'autant plus discutés... que la discussion intéresse peu le *Common Lawyer*. La littérature académique fonde tantôt la *Privacy* sur le droit de propriété qu'aurait chacun sur sa propre personne, conception tirée du philosophe anglais John Locke, et sa célèbre expression « *Every man has his own property on his person* », tantôt sur la défense des libertés, en mettant en avant le fait que la *Privacy* n'existe pas en dictature – *Big Brother* ignore la vie privée – tantôt enfin sur la domination de l'homme sur la femme ainsi que le courant féministe anglais le soutient[20].

18. La Privacy se distingue en toute hypothèse par différents caractères. Elle présente tout d'abord un caractère patrimonial partiel. Une partie de l'identité de la personne qu'elle protège est monnayable, l'image professionnelle par exemple, l'autre ne l'est pas, la dignité par exemple. Elle présente ensuite un caractère limité. La *Privacy* ne fait pas de la personne l'*Homme invisible* de Wells, ou le *Robinson Crusoe* de Defoe[21]. Elle ne protège que contre un niveau variable d'accessibilité de l'information, et n'offre aucune prérogative à la solitude absolue.
Elle présente, enfin, et surtout, un caractère fragile. Elle est en effet constamment attaquée, et constamment réduite. Certains parlent aujourd'hui de la fin de la vie privée, phénomène déjà annoncé en son temps par Bruno Bettelheim[22].

Section 2- La tradition anglaise de la privacy

19. La *Privacy* en droit anglais est conçue de façon fort simple : elle n'existe pas en tant que telle. Seules existent des actions (remedies) mobilisables pour défendre in casu une offense à la vie privée. La Privacy est un thème du droit anglais, non un mécanisme de celui reconnu en tant que tel.

I- L'unité d'esprit

A-La tradition judiciaire

---

18 Op. cit., p. 13
19 Economic Analysis of the Law, Aspen publisher, 1997, p. 46
20 P. Boling, Privacy and the Politics of Intimate Life, Cornell University Press, 1996
21 D. Solove, op. cit., p. 29
22 The Right to Privacy is a Myth, Saturday Evening Post, Jul 27th 1968

20. Il n'existe pas en Angleterre de droit général à la *Privacy*. Les affaires *Malone v/ Metropolitan Police Commissioner* (1979)[23] et *Kaye v/ Robertson* (1991)[24] sont emblématiques de cette lacune volontaire.Dans l'affaire *Malone*, il fut jugé que les écoutes téléphoniques n'enfreignaient pas la *Privacy* de la personne, lorsqu'aucun *Statute* ne réglemente en particulier ce type d'écoutes. Dans l'affaire *Kaye*, un acteur anglais, avait été hospitalisé à la suite d'un accident de voiture. Alors qu'il se reposait après une opération chirurgicale importante, plusieurs journalistes du magazine *The Sunday Sport* s'étaient introduits dans sa chambre d'hôpital malgré l'interdiction de déranger le malade. Ils lui avaient posé différentes questions et réussi à prendre plusieurs photos de l'acteur avant d'être renvoyés de l'hôpital par le médecin. Afin d'empêcher la publication de l'article de presse et des photos, un ami de M. Kaye avait alors intenté, au nom de ce dernier, une action en justice, pour saisir le journal en question. La *Court of Appeal* avait interdit la publication de l'article et des photos, mais de façon indirecte sur la base du délit de *malicious falsehood*. L'absence d'une protection directe de la vie privée fut à cette occasion soulignée et déplorée.

21. La raison d'une telle absence de droit général tient à deux raisons. La première de ces raisons est la structure même du droit anglais qui privilégie traditionnellement la casuistique judiciaire à la construction *ab alto* d'un ordre juridique codifié (*remedies precede rights*). La seconde raison résulte de la volonté des juges de ne pas *créer* un droit de la *Privacy* eux-mêmes, cette tâche revenant au Parlement britannique dont la compétence n'a pas à être l'objet d'empiètement. C'était l'opinion du juge Megarry dans l'affaire *Malone*.

22. Cette position traditionnelle est toujours d'actualité. Comme il se doit en Angleterre, la règle ancienne demeure. Les développements n'ont pas effacé celle-ci. La conception anglaise de la *Privacy* est donc particulariste, et non essentialiste, par tradition. Cette position fut par exemple rappelée dans l'affaire *Nolan v/ Khan* jugée par la Chambre des Lords en 1997[25]. Les juges écrivent ainsi: "*This brings one back to the fact that, under English law, there is in general nothing unlawful about a breach of privacy*". 2

23. De la même façon, il n'y a pas en droit anglais de droit à l'image : *Sport Press Agency v/ Our Dogs* (1916)[26]. La protection de l'image de la personne est assurée contre les photographies ou films de la personne sur la base de la loi sur le *Copyright, Designs and Patent Act* (1988), en tant que défense du droit à la propriété intellectuelle, lorsque la personne a donné son autorisation et n'a pas été rémunérée comme il se devait conventionnellement. Il faut dire qu'il y a au Royaume Uni 4.2 millions de caméras... Plus, en proportion, qu'à Monaco.

24. Des propositions ont déjà été faites pour introduire la *Privacy* en tant que droit général. Ces propositions n'ont jamais abouti, que ce soit en 1972 ou en 1993, où des comités de réflexion avaient été constitués à cette fin. A chaque fois revient la même opposition de principe au zélateur de la *Privacy* : *it's not an English way of doing things*[27].

---

23 Ch 344
24 FSR 62
25 A.C. 558
26 2 KB 880
27 Report of the Committee on Privacy, 1972, Cmnd 5012

25. En conséquence à cela, la *Common Law* anglaise est essentiellement réactive et fragmentée. Réactive, car elle ne conçoit que la défense et non l'affirmation préventive. Fragmentée, car il n'existe pas d'action en justice spécifique à la défense de la Privacy. Il n'y a pas de *Tort of Infringement of Privacy* comme l'ont déjà affirmé les juridictions anglaises : *Wainwright v/ Home Office* (2001)[28]. Là encore, la création d'une action spécifique s'est toujours heurtée à la tradition.

26. Malgré tout, certains points communs relient les différentes actions en justice mobilisées pour défendre la *Privacy*. Le premier point commun réside dans le caractère essentiellement horizontal de la protection offerte. Il s'agit de protéger les individus contre l'ingérence de la Couronne dans leur sphère privée, pas de réglementer les relations entre individus eux-mêmes.

Le second point commun consiste en une tendance générale à retenir une règle *De minimis* et une règle *De maximis*. Dans le premier cas, il s'agit de considérer qu'une action n'est pas envisageable pour se plaindre de l'infraction négligeable à la vie privée : *M v/ Secretary of Work and Pensions* (2006)[29]. Dans le second, il s'agit de considérer que les comportements les plus choquants ne sont pas nécessairement protégés par la *Privacy*, eu égard à leur déviance : *R v/ G* (2008)[30]. Comme l'écrit le juge Hale dans cette affaire: "*Every sexual relationship, however brief or unsymmetrical is* [not] *worthy of respect, nor is every sexual act which a person wishes to perform*".

Le troisième point commun réside quant à lui dans le refus de protéger, sauf cas bien particulier, tout ce qui survient dans un espace public. La *Privacy* est donc liée à l'espace qu'occupe la personne. Par exemple, la jurisprudence anglaise considère que les conditions de traitements d'un SDF n'entrent pas dans le champ de la *Privacy*, pas davantage que la chasse à courre : *Orejudos v/ Kensington and Chelsea* (2003)[31] & *R v/ Attorney General* (2008)[32]. En revanche, le traitement médical est inclus dans la *Privacy*, même délivré à l'hôpital public. Sont aussi protégés ès qualités, pêle-mêle, la solitude, la dignité, l'intégrité morale, les relations sociales non publiques, le domicile et la réputation : *W v/ Westminster* (2005)[33].

B-La protection apportée par le Human Rights Act (1998)

27. L'adoption par le Parlement britannique du Human Rights Act en 1998 a changé le droit anglais profondément. Par cette loi, les juges sont invités à intégrer les droits reconnus par la CEDH dans leur propre raisonnement. S'ils constatent une contrariété entre une loi anglaise et la CEDH, ils sont invités à rédiger une déclaration d'incompatibilité à l'adresse du Parlement, à Westminster. Ce dernier décide, alors, s'il y a lieu, de modifier le Statute en question, au terme d'une procédure d'urgence dite de l'Order.

---

28 3 All E.R. 943
29 2 . AC91
30 1 WLR 1379
31 All ER (D) 369
32 1 AC 719
33 1 FLR 816

28. Ainsi entendu, le HRA comporte, si on l'observe d'un point de vue continental, trois particularités. D'abord, il ne confère pas au juge le pouvoir d'écarter une loi contraire à la CEDH, ce qui revient à le limiter dans son office. Tout au plus peut-il sur la base de la CEDH écarter un règlement. Ensuite, son objet est de protéger les sujets de Sa Majesté contre l'ingérence des autorités publiques, et non, sur un mode vertical, de donner une effectivité inter partes aux droits fondamentaux. Il protège donc essentiellement les personnes privées contre la communication des données personnelles par les administrations. Enfin, le HRA est interprété rétrospectivement par les juges comme l'expression extérieure de ce qui existait déjà à l'état latent dans la Common Law, ce qui revient à en limiter l'éventuelle force novatrice de celle-ci et invite au conservatisme prudentiel. La situation est donc inverse à celle du droit continental en général, et du droit français en particulier. Dans le cas particulier de la Privacy, l'insertion de l'article 8 de la CEDH dans l'ordre juridique anglais aurait théoriquement pu faire émerger un droit général à la Privacy. Cela n'a pas été le cas, comme on pouvait s'y attendre : *Wainwright v/ Secretary of State for the Home Department* (2004)[34]. Le juge anglais considère dans cette décision que les éventuelles lacunes du droit anglais par rapport à l'interprétation donnée par la Cour de Strasbourg de l'article 8 de la CEDH peuvent être comblées par une application affinée des mécanismes déjà existants : *« Sometimes the perceived gap can be filled by judicious development of an existing principle ».*

29. En écho à cette conception restreinte de la Privacy, le Parlement britannique a adopté pour réglementer le statut de la presse écrite dans ce domaine le *Freedom of Information Act* (2000). Un *Code of Practice* (simple Code de conduite, sans valeur légale *stricto sensu*), élaboré par une autorité administrative, la *Press Complaints Commission*, a suivi cette adoption. La version actuelle de ce texte date de 2007. Elle comporte une disposition sur le respect dû à la vie privée. Par ces deux textes, les tribunaux sont invités à mettre en balance l'article 8 et l'article 10 de la CEDH, en tenant compte du *CoP*, lors de la mise en œuvre des mécanismes classiques du droit anglais de la responsabilité: *Douglas v/ Hello !* (2001)[35], et à tenir compte le cas échéant des effets collatéraux de l'atteinte à la Privacy, notamment à l'égard de la famille de la personne : *Maxine Carr v/ News Group Newspapers* (2005)[36].
Ultérieurement, une loi sur la télévision et la radio, le *Communications Act* (2003) a été elle aussi adoptée, avant l'adoption d'un Code de conduite idoine: l'*Ofcom Code.*

Ces deux lois ont essentiellement pour fonction de donner effet aux Codes de conduite et d'éclairer les mécanismes traditionnels de la Common Law. Il s'agit en quelque sorte de *Soft Law* à finalité interprétative ou complétive[37].

II- La diversité des actions

30. Pour défendre la Privacy, la plupart des *remedies* sont des actions en responsabilité. Il s'agit des actions ordinaires du droit de la responsabilité civile (*Tort Law*). Quelle que soit l'action envisagée, certaines conditions invariantes doivent impérativement être respectées :

---

34 EWCA (Civ) 2081, [2003] 3 All E.R. 943

35 2001 QB 967

36 EWHC 971 ; CC v/ AB 2006 EWHC 3083

37 La Press Complaint Commission n'a qu'un pouvoir de médiation. Elle peut ordonner toutefois la publication d'un avis dans la presse, mais ne peut condamner une partie à verser des dommages et intérêts. Ses décisions sont toutefois susceptibles d'appel devant le juge. L'essentiel de la protection découle donc bien du Tort Law.

- Il doit y avoir un dommage
- Il doit exister une action appropriée
- Il ne doit pas s'agir de faire exécuter de force un contrat.

Par ailleurs, et comme en droit des contrats, la situation des plaideurs est toujours appréciée de façon objective. L'intention ou la psychologie des parties n'entre pas en principe en ligne de compte ; et ce, pour des raisons de sécurité juridique. « *The Devil himself knows not the intent of a man* » a-t-on l'habitude de dire en Angleterre[38].

Enfin, certains paramètres moraux influent sur l'appréciation de l'existence d'un *Tort*. C'est le cas du caractère blâmable du comportement du demandeur que peut révéler l'information[39], de son intérêt pour la bonne information du public en général, ou à l'inverse de celui du comportement du défendeur, notamment lorsqu'il est mû par une intention lucrative : *Murray v/ Big Pictures* (2008)[40].

NB : Dans l'affaire *Murray*, des journalistes avaient photographié l'enfant de l'écrivain JK Rowling en train de monter dans un bus, pour vendre la photographie à des *Tabloids*. Il fut jugé qu'il y avait atteinte à la Privacy, car l'esprit de lucre ne pouvait qu'ouvrir la voie à une répétition du comportement.

31. Au-delà de ces points communs, c'est la diversité qui règne. L'action ordinaire du droit de la responsabilité, le *Tort of Negligence*, étant exclue en la matière, les différents *Torts* utilisés en la matière sont les suivants :

- Le Tort of Breach of Confidence
- Le Tort of Trespass
- Le Tort of Nuisance
- Le Tort of Harrassment
- Le Tort of Defamation[41].

A-Le Breach of Confidence

---

38 Brogden v Metropolitan Railway Company (1876–77) L.R. 2 App. Cas. 666. L'expression remonte au XVème siècle

39 Initial Services v/ Putterill [1968], où il était question de la corruption de fonctionnaires.

40 EMLR 12

41 Le Tort of Negligence est exclu, car la jurisprudence considère qu'il n'y a aucun duty of care à l'égard de la Privacy d'autrui. Je dois donc m'abstenir de servir une bière à l'amie de mon client, lorsqu'elle contient un escargot décomposé (v. ainsi le célèbre cas Donhogue v. Stevenson [1932]) mais pas en soi d'enquêter sur la vie privée de celle-ci...

32. Ce *Tort* a été institué initialement pour sanctionner celui qui abuse de la confiance d'autrui et provoque par là un dommage. Il a été mobilisé en 1848 pour faire condamner un éditeur qui avait publié des dessins réalisés par le Prince Albert, et dix ans plus tard pour faire interdire à un photographe de publier ou de vendre les photographies d'un modèle sans son autorisation : *Prince Albert v/ Strange* (1849)[42] & *Pollard v/ Photographic Company* (1888)[43].

33. Ce *Tort* est utilisé dans le contexte de la Privacy pour créer une action spécifique d'abus de l'information (*misuse of information*). Dans sa mise en œuvre, il invite le juge à mettre en balance les articles 8 et 10 de la CEDH : *Campbell v/ MGN* (2004)[44].

34. Pour qu'il y ait ainsi *misuse of information,* 3 conditions doivent être réunies :
- L'information doit avoir été transmise dans le cadre d'une relation de confiance
- Elle doit avoir transmise sous le sceau du secret
- Il doit y avoir divulgation non autorisée (*Coco v/ Clark* [1969][45]).

35. Une relation de confiance existe ainsi, selon la jurisprudence, entre un médecin et son patient, un journaliste et sa source, ou entre les parties à une relation sexuelle : *Barrymore v/ News Group Newspaper* (1997)[46].

36. La confidentialité peut être contractuellement stipulée, mais l'obligation peut découler des circonstances hors tout contrat : *Stephens v/ Avery* (1988)[47] ; *Queensbarry v/ Shebbeare* (1761)[48], où le juge avait estimé qu'il y avait une obligation de confidentialité dans le chef du récipiendaire d'un manuscrit.
Elle peut découler tout autant de la nature même de l'information, comme c'est le cas pour la jurisprudence du secret d'affaire, du secret marital, du secret sexuel, des confessions artistiques ou du secret de la correspondance.
En revanche, l'information n'a pas à être intime. Elle peut être économique ou stratégique : ●*BC v/ MGN* (2004)[49] & *Spycatcher*[50].
Enfin, les circonstances de la collecte de l'information influent sur l'appréciation de sa confidentialité[51]. L'intention de l'auteur de la divulgation est ici prise en considération.

B- Le Tort of Trespass

37. L'action de *trespass* sanctionne le fait de pénétrer dans le domicile d'une personne sans autorisation, d'y rester sans permission ou après l'expiration de celle-ci.
Le domicile, dans ce contexte, n'est pas nécessairement une propriété. Le titre légal de l'occupant n'est pas en soi déterminant : *Qazi v/ London Borough of Harrow* (2004)[52].

---

42 1 Mac. & G. 25
43 Ch. p. 345
44 UKHL 22
45 R.P.C. 41
46 FSR 600
47 1 Ch. 449
48 3 Eden 32. Dans cette dernière affaire, il fut jugé que le récipiendaire d'un manuscrit avait une obligation de confidentialité.
49 1 AC 1
50 Attorney-General v Observer Ltd [1990] 1 A.C. 109
51 Richard Clayton & Hugh Tomlinson, op. cit., p. 15

L'intrusion, quant à elle, doit être bien réelle. Elle peut être physique, ou immatérielle, par exemple par l'installation de microphones ou par la pénétration par le bruit : *Greig v/ Greig* (1966)[53] & *Dennis v/ Ministry of Defence* (2003)[54]. En revanche, la simple observation du domicile depuis l'extérieur n'est pas un *trespass* : *Bernstein v/ Skyways* (1978)[55]. Dans cette affaire, des photographes avaient survolé par les airs une maison pour la photographier. L'espionnage sans intrusion n'est donc pas un *tresspass*, car les yeux ne sont pas en eux-mêmes intrusifs. Comme l'écrit le juge dans l'arrêt *Entick v/ Carrington* (1765)[56] : *The eye cannot by the laws of England be guilty of a trespass* En revanche, il peut y avoir le cas échéant harcèlement.

C- Le Tort of Nuisance

38. Cette action protège les citoyens contre les troubles intolérables et prolongés affectant l'utilisation d'une propriété. Elle a permis, dans quelques rares hypothèses, d'offrir une protection indirecte de la vie privée. Mais son importance dans ce domaine est extrêmement limitée, principalement en raison du fait que l'atteinte doit être prolongée et que la protection n'est accordée qu'au propriétaire du terrain.

39. A titre d'exemple, dans l'affaire *Walker v. Brewster* (1876)[57], des propriétaires ont pu obtenir sur cette base la condamnation d'un voisin qui avait fréquemment organisé de grandes soirées bruyantes et dérangeantes pour l'entourage, en mettant en avant le fait que ces soirées envahissait leur vie nocturne et constituait de ce fait une atteinte à leur vie privée.

D- Le Tort of Harrassment

40. La victime d'une atteinte à l'image peut éventuellement agir sur le terrain du harcèlement en fondant son action sur le *Protection Harrassment Act* (1997).

41. Pour qu'une telle action aboutisse, il faut que le harcèlement soit constitué, c'est-à-dire que deux conditions soient remplies :
- Il doit y avoir pluralité d'atteintes
- Cette pluralité doit avoir provoqué un dommage.

42. Contre une telle action, le défendeur peut imposer le standard de raison (*reasonableness*), pour opposer que son comportement n'est pas hors du commun au vu des circonstances.

43. Dans le domaine qui nous occupe, cette action ne joue pas un rôle prépondérant.

Section 3 - Les tendances contemporaines

44. Nonobstant la diversité de ses moyens d'action, le droit anglais connaît certains développements récents qui le rendent plus accessible à l'idée même d'un droit à l'oubli. Ces

---

52 1 AC 983
53 VR 376
54 Env LR 34
55 1 QB 479. Une photographie d'une propriété privée avait prise depuis les airs…
56 EWHC KB J98
57 LR 5 Eq 25

développements, qui se retrouvent aussi bien en jurisprudence qu'en législation, sont particulièrement mis en lumière par la récente affaire Mosley.

I-Les tendances contemporaines en jurisprudence

45. La jurisprudence anglaise n'est pas entièrement réfractaire à l'idée d'un développement d'un mécanisme d'oubli, ou plus simplement de recul de l'information, lorsque la protection de la Privacy de la personne le requiert.

46. Ainsi, la jurisprudence tend à étendre le champ de la protection de la Privacy de la personne aux relations que cette dernière entretient avec d'autres personnes privées. Autrement dit, la Privacy n'est plus seulement un rempart contre l'ingérence publique dans l'intimité du sujet, mais un mécanisme plus général apte à produire des effets horizontaux. C'est notamment l'opinion de Lord Hoffmann que consigne l'arrêt Campbell v/ Mirror Group Newspaper (2004)[58].

47. De la même façon, la jurisprudence tend à étendre potentiellement la sphère de protection de la Privacy en l'ajustant en fonction des circonstances.
A ce titre, les Cours anglaises tendent tout d'abord à étendre le champ de la Privacy à des faits survenus dans l'espace public. La jurisprudence a par exemple considéré que le simple fait de prendre le bus pouvait être considéré comme un fait privé : *Murray v/ Big Pictures* (2008)[59]. Le caractère trivial de l'information n'exclut pas de la même façon qu'elle relève de la *Privacy* : *Lord Browne v/ Associated Newspapers* (2008)[60].
Ensuite, la jurisprudence récente admet aujourd'hui que le partage d'une information avec plusieurs personnes, par exemple sur un réseau social, ne rend pas pour autant ladite information *publique*. Dès lors, le fait pour une des personnes destinataires de l'information de divulguer celle-ci au-delà du cercle des destinataires choisis initialement en la publiant de façon plus large peut constituer un *breach of confidence* : *Lord Browne of Madingley v/ Associated Newspaper* (2008)[61]. Il y a donc là un moyen d'action contre la mise en circulation élargie et abusive d'une information, et l'admission d'une sphère de *Privacy* choisie unilatéralement par la personne.
Enfin, et surtout, la jurisprudence anglaise considère désormais qu'une information n'est pas publique par nature *sub specie aeternitatis*. Une information considérée à un moment comme publique peut dont avec le temps perdre son intérêt pour la collectivité et redevenir privée, ce qui constitue ni plus ni moins que la base théorique d'un droit à l'oubli : R *v/ Broadcasting Complaints Commission* (1995)[62] & R *v/ Chief Constable of North Wales Police* (1999)[63]. Cette possibilité de translation du secteur public à la *Privacy* est d'ailleurs réversible et à double sens, car une information privée peut aussi devenir publique avec le temps, comme il a été jugé à l'égard de conversations privées tenues au Cabinet d'un ministre il y a 10 ans et valablement publiées

58 2 AC 457
59 EMLR 12
60 QB 103
61 Préc.
62 EMLR 163
63 QB 396

aujourd'hui dans un but informatif : *AG v/ Jonathan Cape* (1976)[64]. La jurisprudence mitige aussi le champ de la liberté d'expression dans sa relation de faits intimes. Elle considère parfois que la relation par écrit de la commission d'un adultère est admissible, tandis que la publication d'une photographie prise en flagrante luxure sort du champ de la liberté d'expression : *John Terry v/ Persons Unknown* (2010)[65].

II-Les tendances contemporaines en législation

48. Le *Data Protection Act* (1998) règlemente la collecte et la centralisation des données personnelles par tout système d'information organisés[66]. Il constitue la transposition anglaise de la directive de l'Union sur les données personnelles de 1996.

49. ●r, ce texte institue au bénéfice de toute personne dont les données figurent au fichier concerné un *droit d'effacement*, lorsqu'il est démontré soit que l'information est inexacte ou imprécise, soit que son usage et son maintien causerait à la personne un dommage certain (*substantial damage*). Bien évidemment, le texte n'ouvre pas par là la voie à un effacement *ad nutum*. Toutefois, la base même d'un effacement d'une donnée dont il n'est pas démontré que son inscription est justifiée par des raisons valables est ici posée. L'institution d'un droit à l'oubli pourrait parfaitement s'appuyer sur un tel mécanisme[67].

50. A l'inverse, le maintien et la communication des données personnelles sont au contraire d'autant plus facilement admise que les données en question ont été *anonymisées*, et ne permettent plus par conséquent d'identifier la personne et donc de lui causer un dommage : *Sayers v/ Smithkline Berecham* (2007)[68].

51. La question de l'institution d'un droit à l'oubli reposant techniquement sur un effacement de l'information n'est donc pas si étrangère que cela aux mécanismes du droit anglais. L'affirmation est d'autant plus sérieuse, que des voix se sont faites entendre en Angleterre en faveur de l'application à *Google* du *Data Protection Act* (1998), notamment lorsque des caméras de l'entreprise ont sillonné les rues d'Angleterre pour mettre en place la fonction *Google Street View*. Cette application serait justifiée spatialement par le fait que le DPA s'applique à tout système

---

64 1 QB 752

65 EWHC 119

66 S1 [1]

67 Le Data Protection Act institue ainsi dans son article 10 un Right to prevent processing likely to cause damage or distress. Le texte dispose à ce titre : "(1)Subject to subsection (2), an individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the ground that, for specified reasons—
(a)the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another, and
(b)that damage or distress is or would be unwarranted". Et l'article 14 (1) institue quant à lui un droit d'effacement des données inexactes. Le texte dispose : " If a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contain an expression of opinion which appears to the court to be based on the inaccurate data ".

68 WHC 1346

d'information établi au Royaume Uni, ou ayant des établissements secondaires sur le territoire du royaume à partir desquels des informations transitent (article 5 du DPA)[69].

III- L'affaire Mosley (2008)

52. L'affaire *Mosley* pourrait peut-être, de l'aveu même des auteurs anglais, constituer un tournant dans l'histoire de la *Privacy* anglaise.
En l'espèce, le président de la Fédération internationale de formule 1, *Max Mosley*, avait été filmé à son insu au cours d'une orgie sadomasochiste par une des prostituées recrutées pour l'occasion. L'orgie en question comportait des éléments de mise en scène reprenant des symboles nazis. Les prostituées, vêtues d'un uniforme gris, lui donnaient ainsi des ordres en allemand, avant de revêtir des pyjamas rayés pour se faire cravacher par l'intéressé. La vidéo avait été postée sur internet par le journal *The News of the World*, avant d'être vue plus d'1.4 millions de fois. *Mosley* avait attaqué le journal pour *breach of confidence*, la scène s'étant déroulée dans un lieu entièrement privé. Il obtint gain de cause et le journal fut condamné à lui verser 450 000 £. Or la décision rendue par le juge anglais[70] ne fut pas basée à proprement parler sur la théorie du *breach of confidence*, mais directement sur l'article 8 de la CEDH. Le juge estima en effet que la mise en scène nazi était équivoque et non certaine, et que l'affirmation du journal selon laquelle *Mosley* était un pervers néonazi excédait par conséquent le champ de la liberté d'expression en empiétant sur la vie privée protégée par l'article 10 de la CEDH. Or un tel raisonnement opère une *tabula rasa* des mécanismes traditionnels de la *Common Law* anglaise, pour affirmer via la CEDH l'existence d'un véritable droit à la *Privacy* ; et ce, à rebours de la tradition anglaise[71]. Or une telle évolution, si elle venait à être confirmée, irait dans le sens d'un renforcement de la protection de la *Privacy* et pourrait abaisser le niveau de résistance intrinsèque du droit anglais à l'émergence d'un droit à l'oubli. Ultérieurement, *Mosley*, ruiné professionnellement, a attaqué le Royaume Uni devant la CEDH en invoquant le fait que le droit anglais aurait dû imposer au journal une obligation d'informer la personne de son intention de publier une information scabreuse de nature privée, pour éviter une publication indélébile que des dommages et intérêts ne peuvent réparer complètement, le trouble ne cessant jamais. Il fut débouté par l'arrêt *Mosley v/ Royaume Uni* (2011)[72], la Cour considérant que la Convention laisse aux Etats le soin d'instituer s'ils le souhaitent une telle obligation de prévenir, rien dans la Convention n'imposant le recours obligatoire en droit national à un tel mécanisme[73].

Conclusions

En résumé, le droit anglais ignore par tradition le concept de *vie privée* au sens où le droit continental l'entend. Il ne connaît initialement que des remèdes particuliers pour faire cesser,

---

69 V. ainsi en faveur de l'application du DPA à Google, jugé peu respectueux de la Privacy : Brian Glick, Google privacy policy 'does not meet' EU data protection laws, in : Computer Weekly, 28 février 2012. www.computerweekly.com/news/2240118608/Google-privacy-policy-does-not-meet-EU-data-protection-laws

70 Mosley [2008] EWC 1777

71 James E. Stanley, Max Mosley and the English Right to Privacy, 10 Wash. U. Glob. Stud. L. Rev. 641 (2011)

72 Mosley v United Kingdom [2011] 53 E.H.R.R. 30

73 De fait, ladite vidéo continue de circuler, plus de 5 ans après. A ce jour, elle est toujours disponible gratuitement en version incomplète sous la forme d'un best of, et en version uncut sur des sites spécialisés dans la publication de vidéos pornographiques réelles et volées et reposant sur des appels à publication à titre onéreux...

dans les conditions du droit commun de la responsabilité civile, le trouble à ce que nous appelons en droit civil la vie privée, et protège davantage que nous la liberté d'expression, y compris dans son exerce intrusif. Cette tradition est toutefois remise en cause par une évolution récente qui, par le biais du droit de l'Union européenne ou de la CEDH, tend à faire admettre un véritable droit à la vie privée autonome et substantivé. Dès lors, au-delà des paramètres de circonstances introduisant à l'occasion une prise en compte du nécessaire *oubli* de l'information personnelle au sein de la tradition juridique, l'institution d'un droit à l'oubli à l'échelle européenne n'est nécessairement impossible du point de vue britannique, pour autant que cette institution s'insère dans les mécanismes anglais existants et ne passe pas par l'imposition d'un droit général à l'effacement *ad nutum*.

En conséquence, 4 options semblent théoriquement envisageables pour instituer un droit à l'oubli :

- Option I : Ne rien faire, et laisser la soft law autant que la jurisprudence anglaise régler le problème ;
- Option II : Instituer un droit à l'oubli limité et exceptionnel en droit de l'UE, en laissant aux droits nationaux le soin de prévoir ses modalités de mise en œuvre via leurs propres instruments existants ou non ;
- Option III : Instituer un droit à l'oubli limité et exceptionnel en droit de l'UE, en définissant son contenu autant que la ou les nouvelles actions idoines instituées ès qualités pour garantir sa mise en œuvre ;
- Option IV : Instituer un droit à l'effacement général sur le mode d'un droit à l'autodétermination informationnelle.

Eu égard aux contraintes techniques du web d'une part et à la tradition anglaise d'autre part, les options II et III semblent les plus acceptables si l'on souhaite une intervention du droit européen en la matière.

CHAPITRE 2

Sens et possibilités d'un « droit à l'oubli » aux États-Unis[1]

« J'ai à moi seul plus de souvenirs que n'en peuvent avoir eu tous les hommes depuis que le monde est monde [...]
Mes rêves sont comme votre veille [...]
Ma mémoire, monsieur, est comme un tas d'ordures »

(Jorge Luis Borges, « Funes ou la mémoire »)[2].

« J'ai plus de souvenirs que si j'avais mille ans.

Un gros meuble à tiroirs encombré de bilans,
De vers, de billets doux, de procès, de romances,
Avec de lourds cheveux roulés dans des quittances,
Cache moins de secrets que mon triste cerveau.
C'est une pyramide, un immense caveau,
Qui contient plus de morts que la fosse commune.
— Je suis un cimetière abhorré de la lune,
Où comme des remords se traînent de longs vers
Qui s'acharnent toujours sur mes morts les plus chers.
Je suis un vieux boudoir plein de roses fanées,
Où gît tout un fouillis de modes surannées,
Où les pastels plaintifs et les pâles Boucher
Hument le vieux parfum d'un flacon débouché ».

(Charles Beaudelaire, « Spleen » LXXVI)[3]

---

1 Par Fabien Girard, Maître de conférences à la faculté de droit de Grenoble.
2 J.L. Borges, « Funes ou la mémoire », in J.L. Borges, Fictions, Folio, Paris, 1983, p. 109-118, spéc. p. 115.
3 Ch. Beaudelaire, Les fleurs du mal, in Œuvres complètes, I, Gallimard, La Pléiade, Paris, 1975, p. 73 et s.

Introduction

1. Renversé par un cheval dans l'estancia de San Francisco à Fray Bentos, Uruguay, le jeune Funes se retrouve paralysé, mais doté d'une mémoire prodigieuse : « Dans sa chute, il avait perdu connaissance ; quand il était revenu à lui, le présent ainsi que les souvenirs les plus anciens et les plus banals étaient devenus intolérables à force de richesse et de netteté. Il s'aperçut peu après qu'il était informe. Le fait l'intéressa à peine. Il estima (sentit) que l'immobilité n'était qu'un prix minime. Sa perception et sa mémoire étaient maintenant infaillible ». Le narrateur de la nouvelle de Borges en témoigne : « Il avait appris sans effort l'anglais, le français, le portugais, le latin » ; mais il ajoute immédiatement : « Je soupçonne cependant qu'il n'était pas très capable de penser. Penser c'est oublier des différences, c'est généraliser, abstraire. Dans le monde surchargé de Funes il n'y avait que des détails, presque immédiats »[4].

Les cas d'hypermnésie pathologique sont aujourd'hui bien documentés[5] et viennent confirmer les troubles remarquables de Funes qu'avait déjà aperçus Nietzche. Car s'il est un « mauvais oubli », ce qu'on pourrait appeler une lésion de mémoire, il est aussi et surtout un « oubli positif » qui est le privilège des « natures pleines et fortes, en qui se trouve en surabondance la force plastique et régénératrice qui permet de guérir et même d'oublier »[6]. L'oubli n'est pas (ou pas seulement) *force d'inertie* (*vis inertiae*) ; bien plutôt « pouvoir actif, une faculté d'inhibition positive au sens le plus strict du mot, faculté à laquelle il faut attribuer le fait que tout ce qui nous arrive dans la vie, tout ce que nous absorbons se présente tout aussi peu à notre conscience pendant l'état de "digestion" (on pourrait l'appeler une absorption psychique) que le processus multiple qui se passe dans notre corps pendant que nous "assimilons" notre nourriture »[7]. L'oubli (oubli « positif ») est donc bien une qualité essentielle, et comme nous prévient le philosophe allemand : « [n]ul bonheur, nulle sérénité, nulle espérance, nulle fierté, nul instant présent ne pourraient exister sans faculté d'oubli »[8].

2. Loin de s'opposer, mémoire et oubli se complètent. « Force vive » de la mémoire, l'oubli vient « façonner » les traces mnésiques et souvenirs comme « les contours du rivage de la mer »[9] ; c'est l'oubli qui assure la « mise en fiction » de la vie individuelle et collective – qui assure la construction des identités[10]. Entre « assimilation » (*ars memoriae*) et « digestion » (*ars oblivionis*), l'équilibre mémoriel se dessine généralement de lui-même, traçant en chemin les linéaments d'une mémoire individuelle et collective, écrivant en route les premières pages d'un récit biographique

---

4 J.L. Borges, op. cit., p. 118.

5 Cf. E.S. Parker, L. Cahill, J.L. McGaugh, « A Case of Unusual Autobiographical Remembering », Neurocase 12 (2006), p. 35-49 ; v. aussi V. Mayer-Schönberger, Delete.- The Virtue of Forgetting in the Digital Age, Princeton University Press, Princeton, Oxford, 2009, p. 12-13.

6 F. Nietzche, « La généalogie de la morale », in Œuvres, éd. par Jean Lacoste et Jacques Le Rider, Robert Laffont, éd. Bouquins, Paris, 1993, p. 789 (cité par J. Le Rider, « Oubli, mémoire, histoire dans la "Deuxième Considération inactuelle" », Revue germanique internationale 11 | 1999, n° 7).

7 F. Nietzche, « La généalogie de la morale », op. cit., Deuxième dissertation, § 1, p. 803 (J. Le Rider, op. cit., loc. cit.).

8 F. Nietzche, op. cit., loc. cit.

9 M. Augé, Les Formes de l'oubli, Rivages poche, Paris, 2001, p. 29-30.

10 M. Augé, op. cit., p. 47 ; P. Ricœur, La mémoire, l'histoire, l'oubli, Éditions du Seuil, Paris, 2000, p. 574 et s.

et d'un roman national[11] ; processus subtil assurément, marqué par les figures complexes (de l'oubli) du *retour*[12], du *suspens*[13] et du *commencement*[14], jamais réellement conscient sauf, peut-être, lorsque l'État prend à sa charge le « devoir de mémoire »[15] ou encore (et en sens inverse) aménage la prescription ou l'amnistie[16]. L'oubli est, en tout cas, indéfectiblement attaché au présent : c'est en lui que le passé se perd ou se retrouve ; c'est en lui que le futur s'esquisse[17]. Il lie aussi solidement trajectoires individuelles et collectives. C'est que les institutions « emblématiques » de l'oubli ont toujours une double signification : *épreuve individuelle* et *événement social*. Et même si ces significations ne coïncident pas nécessairement (l'oubli du passé pour l'individu vaut souvenir du rituel d'initiation pour la collectivité), elles rappellent « qu'il faut être au moins deux pour oublier, c'est-à-dire pour gérer le temps »[18]. Bien qu'imbriquant toujours le singulier et le pluriel, les institutions de l'oubli ne sont pas toutes tournées vers les mêmes intérêts. Certaines, comme la prescription ou l'amnistie, entendent protéger l'intérêt collectif ; d'autres, celles dont il va être désormais question, prétendent servir, en premier lieu, l'intérêt individuel[19].

---

11 Sur le roman national français, v. Ph. Joutard, « L'oubli constructeur des mémoires collectives », in F. Dosse, C. Goldenstein (dir.), Paul Ricœur : penser la mémoire, Seuil, Paris, 2013, p. 235-250.

12 La figure du « retour » signifie retrouver un passé perdu en oubliant le présent, ainsi que « le passé immédiat avec lequel il tend à se confondre », et ce afin de « rétablir une continuité avec le passé plus ancien », d'« éliminer le passé "composé" au profit d'un passé "simple" » (M. Augé, op. cit., p. 76). L'exemple est celui de l'institution de la possession en Afrique : « celui qui a été possédé, selon des formes rituelles valables, par un esprit, un ancêtre ou un droit, doit oublier cet épisode dès qu'il s'achève ». C'est la présence « d'un autre en lui » qui « s'efface alors de sa conscience ». Ensuite, le possédé « retrouve ses esprits » (p. 76) – c'est cela la figure du retour, retour du possédé.

13 Le suspens suppose de retrouver le présent « en le coupant provisoirement du passé et du futur et, plus précisément, en oubliant le futur pour autant que celui-ci s'identifie au retour du passé » (M. Augé, op. cit., p. 77). Cette forme d'oubli s'incarne dans les inversions sexuelles ou sociales (l'homme qui joue la femme, l'esclave qui joue le roi). Augé observe : « Celui qui joue le jeu de l'inversion [...] joue à abolir en lui la présence du même et il n'est pas exclu qu'il se prenne au jeu : il n'est plus ce qu'il était et il oublie ce qu'il redeviendra (le même) ou deviendra (un mort, dans le cas de l'esclave destiné à suivre le sort du roi défunt) » (ibid.).

14 L'ambition du commencement est ici de « retrouver le futur en oubliant le passé, de créer les conditions d'une nouvelle naissance qui, par définition ouvre à tous les avenirs possibles sans en privilégier aucun. La forme rituelle emblématique du commencement ou du re-commencement serait l'initiation qui, sous des modalités variables, est toujours présentée comme un engendrement et une naissance. Ce qui s'efface ou s'oublie alors, dans l'instant où surgit une nouvelle conscience du temps, c'est simultanément celui que l'initié n'est plus et celui qu'il n'est pas encore, le même et l'autre en lui » (M. Augé, op. cit., p. 78).

15 R. Letteron, « Le droit à l'oubli », RDP 1996, p. 385 et s. ; D. Truchet, « À propos du droit à l'oubli et du devoir de mémoire », Mélanges en hommage au Doyen Gérard Cohen-Jonathan, Vol. II, Bruylant, Bruxelles, Paris, 2004, p. 1595.

16 Sur ces deux institutions, v. C. Hardoin-Le Goff, L'oubli de l'infraction, LGDJ, Paris, 2008, n° 1 et s. ; H. Matsopoulou, « L'oubli en droit pénal », Mélanges dédiés à Bernard Bouloc, Dalloz, Paris, 2006, p. 771.- Sur les rapports avec le pardon : v. P. Ricœur, La mémoire, l'histoire, l'oubli, op. cit., p. 585 et s., p. 593 et s.

17 M. Augé, op. cit., p. 78-79 : « C'est toujours au présent, finalement, que se conjugue l'oubli : le présent continué (« je suis revenu »), forme présente du passé composé qui, significativement, utilise l'auxiliaire être, verbe d'état ; le présent pur, le pur présent de l'instant (« je suis là ») ; le présent inchoatif qui s'ouvre sur le futur (« je vais partir »). Nous pourrions dire aussi bien que, lorsqu'il s'agit d'oubli, tous les temps sont des temps du présent, puisque le passé s'y perd ou s'y retrouve et que le futur ne fait que s'y esquisser ».

18 M. Augé, op. cit., p. 81.

19 V., en ce sens, A. Marais, « Le droit à l'oubli numérique », in B. Teyssié (dir.), La communication numérique, en droit, des droits, éd. Panthéon-Assas, Paris, 2012, n° 3.

3. En brossant l'histoire de l'humanité à grands traits, on observera que l'homme n'a jamais cessé de chercher à accroître ses capacités de mémorisation. Au-delà de l'apparition du langage, puis de la peinture, c'est bien la naissance de l'écriture qui a bouleversé définitivement les rapports de l'homme à la mémoire[20], en faisant apparaître une première forme efficace de mémoire externe. Mais la révolution ne sera réalisée que bien plus tard, avec l'invention du caractère mobile d'imprimerie typographique qui aura pour effet d'accélérer de manière remarquable le processus de production des copies, tout en abaissant son prix[21]. Le mouvement se poursuivra avec la production de masse et l'apparition de nouvelles mémoires externes que sont les films photographiques, les cassettes audio et vidéo. Aucun de ces derniers événements n'a été anodin du point de vue du sujet qui nous occupe[22]. Mais aucun n'a eu pour effet de remettre en cause ce principe souligné par Viktor Mayer-Schönberger : « pendant des millénaires, oublier est demeuré un peu plus simple et moins cher que se souvenir »[23].

L'invention de l'ordinateur et des mémoires digitales a modifié le paradigme. Dans le monde numérique, la mémorisation de l'information est devenue à la fois simple et peu coûteuse. Sous l'effet de la standardisation, toutes les informations que nous produisons au quotidien – vidéo, son, photographie, texte, etc., dont la constitution et consultation nécessitaient autrefois plusieurs appareils – peuvent désormais être produites et extraites à partir d'un terminal unique (*ordinateur personnel, téléphone portable, tablette, etc.*). Les capacités de stockage d'information ont considérablement crû, tandis que les supports n'ont cessé de se réduire et les prix de baisser. En 1950, le coût de l'unité de stockage était de $70 000 par mégabit ; en 1980, ce coût avait chuté à $500. Vingt ans plus tard, il était ramené à 1 cent et, en 2008, à un centième de cent[24]. Dans le monde digital, il est partant devenu plus cher d'oublier (c'est-à-dire d'effacer) que de mémoriser[25].

4. Tous ces facteurs convergent pour remettre en cause l'équilibre entre *ars memoriae* et *ars oblivionis*. L'oubli étant devenu l'exception, se trouve désormais amplifié, du moins en Europe, le mouvement réclamant la consécration d'un véritable « droit à l'oubli ». Pour autant, le concept, que l'on doit semble-t-il au Professeur Gérard Lyon-Caen[26], qui l'introduisit dans son commentaire de cette célèbre décision ayant opposé la veuve de Landru au réalisateur Claude Chabrol[27], est bien antérieur à l'ère numérique et aux revendications de l'*homo numericus*. Et la

---

20 V. Mayer-Schönberger, Delete.- The Virtue of Forgetting in the Digital Age, op. cit., p. 23 et s.

21 Comme le remarque Eisenstein, entre 1453 et 1503, environ 8 millions de livres sont imprimés, soit sans doute plus que tous les scribes de l'Europe avait réussi à produire depuis la fondation de Constantinople, 1250 ans plus tôt : E.L. Eisenstein, The Printing Revolution in Early Modern Europe, Cambridge University Press, Cambridge, 1993, p. 13.

22 S'agissant de la photographie, v. infra, n° 21.

23 V. Mayer-Schönberger, op. cit., p. 49.

24 V. Mayer-Schönberger, op. cit., p. 63.- La question de la mémoire numérique ne peut être étudiée sans celle de l'Internet, du réseau : cf. G. Finocchiaro, « La memoria della rete e il diritto all'oblio », Il diritto dell'informazione e dell'informatica, Anno XXVI, Fasc. 3 – 2010, p. 391 et s.

25 Op. cit., p. 68.

26 G. Lyon-Caen, note ss. TGI Seine, 14 oct. 1965, JCP G 1966, II, 14 482.

27 TGI Seine, 14 oct. 1965, JCP G 1966, II, 14 482. Dans cette affaire, le tribunal refusait de faire droit à la demande de l'une des maîtresses de Landru qui demandait réparation du dommage prétendument causé par la diffusion du film de Claude Chabrol. C'est que pour le tribunal, cette dernière ayant notamment publié ses mémoires, elle ne pouvait « invoquer à son profit la prescription du silence ». C'est au sujet de cette « prescription du silence » que le

plupart des jugements et arrêts ultérieurement rendus, évoquant fût-ce indirectement la thématique du droit à l'oubli, l'ont été dans un contexte de médias traditionnels. Il ne faudrait certes pas oublier l'autre grande première évocation du droit à l'oubli, faite à l'occasion de la promulgation de la loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés (loi dite « Informatique et libertés »)[28]. Le sénateur Jacques Thyraud, dans son rapport fait en 1977[29], et le Professeur Maisl, dans un commentaire avisé du texte, paru en 1978, voyait déjà dans l'ancien article 28 de la loi, un « droit à l'oubli »[30]. L'expression fut reprise dix ans plus tard, par la CNIL, dans son importance rapport de 1988[31]. Mais disons-le, à cette époque, la loi était destinée à protéger les citoyens contre les fichiers détenus par l'administration et si l'informatique existait bien évidemment, l'Internet n'était encore qu'un projet[32].

La fin du millénaire a dit-on apporté avec elle de nouvelles problématiques et donné au droit à l'oubli une physionomie qu'on lui connaît mieux. C'est l'Internet qui concentre aujourd'hui toutes les attentions et qui vient enrichir le concept d'une épithète : droit à l'oubli « numérique ». La précision est censée circonscrire un problème particulier et augurer d'un régime juridique propre. Est-ce bien le cas ? À la vérité, la plupart des textes invoqués de longue date en Europe pour soutenir le droit à l'oubli sont demeurés à l'identique (article 9 du Code civil, article 8 de la Convention européenne des droits de l'homme (Conv. EDH)) ou n'ont été que marginalement modifiées (L. n° 78-17 du 6 janvier 1978)[33]. Ceux qui sont venus s'ajouter, comme la directive n°

Professeur Lyon-Caen avait évoqué le droit à l'oubli. En appel (Paris, 15 mars 1967, aff. Landru, D. 1967, somm. p. 78, JCP G 1967, II, 15 107), la cour soulignait l'existence de faits déjà « largement » divulgués et estimait que le procès Landru figurait parmi les procès de droit commun « les plus sensationnels du siècle ». Et d'ajouter que « si chacun a, en principe, le droit de s'opposer à la divulgation de faits de sa vie privée, il en est autrement lorsque les faits ont déjà été légalement divulgués et qu'aucune faute ne s'induit des circonstances dans lesquelles la nouvelle divulgation s'est réalisée ». Les magistrats relevaient également que la requérante avait « sollicité plusieurs entreprises de presse pour la publication de ses mémoires », ce qui tendait à prouver qu'elle n'aspirait pas à ce que « le silence se fasse sur la période de sa vie où elle connut Landru ». En conclusion, la société productrice du film n'avait pas « tiré de l'oubli des événements et des personnes sur lesquels il n'est pas tombé ».- V. aussi, TGI Paris, réf. 6 décembre 1979, D. 1980, p. 150, note R. Lindon, au sujet d'une maîtresse de Mesrine qui s'opposait à la publication du livre « Coupable d'être innocent » rédigé par Jacques Mesrine lui-même ; et Civ. 1re, 13 févr. 1985, 2 arrêts, JCP G 1985, II, 20 467, note R. Lindon, à propos d'une autre maîtresse (1re espèce).

28 JORF 7 janv. 1978, p. 227.

29 Rapport n° 72 (1977-1978) de M. Jacques Thyraud, fait au nom de la commission des lois, relatif à l'informatique et aux libertés, déposé le 10 novembre 1977, spéc. p. 6 : « L'informatique a apporté essentiellement un changement de dimension : elle a introduit, en effet, 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 ».- V. aussi les échanges remarquables contenus in Informatique et Libertés, Discussion d'un projet de loi, Sénat, Séance du 17 nov. 1977, JORF année 1977-1978, n° 77 S., p. 2750, p. 2753, p. 2754.

30 H. Maisl, « La maîtrise d'une interdépendance », JCP G 1978, I, n° 2891, spéc. n° 24.- L'ancien article 28 de la loi de 1978 était rédigé comme suit : « Sauf dispositions législatives contraires, les informations ne doivent pas être conservées sous une forme nominative au-delà de la durée prévue à la demande d'avis ou à la déclaration, à moins que leur conservation ne soit autorisée par la commission ». V., aujourd'hui, le nouvel article 6, 5°.

31 CNIL, Dix ans d'informatique et libertés, Economica, Paris, 1988, p. 18.

32 A. Marais, « Le droit à l'oubli numérique », op. cit., spéc. n° 4-5.

33 Cette loi a été principalement modifiée 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 et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (L. n° 2004-801, 6 août 2004, JORF 7 août 14 063).

95/46/CE du 24 octobre 1995[34] ou l'article 8 de la Charte des droits fondamentaux de l'Union européenne[35], ont certes tenu compte des évolutions du monde numérique, mais sans réellement renouveler la méthode. Si des menaces nouvelles sont apparues – comme les réseaux sociaux, l'utilisation des cookies ou bien encore les métadonnées, les données de géolocalisation, la reconnaissance faciale etc. – l'essentiel du contentieux se concentre toujours autour de deux grandes thématiques générales qui n'ont été renouvelées que dans leur ampleur, leur complexité aussi, et peut-être encore par l'acuité nouvelle avec laquelle elles ont été perçues et saisies : la redivulgation d'une information ayant trait à la vie privée et la maîtrise de l'individu sur ses données personnelles.

5. C'est à travers ces deux prismes, avant tout européens[36], qu'il convient de porter un regard sur le droit des États-Unis. Eux seuls sont à même de répondre à la question du *sens* du droit à l'oubli avant de mener une possible comparaison et de donner des indications sur le *possible*. Il serait vain de procéder à rebours, depuis le droit américain qui ne s'est intéressé à cette notion (plus ou moins inconnue jusqu'alors) que parce qu'elle figurait dans la proposition de règlement du Parlement européen et du Conseil 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[37] et que ce texte était de nature à affecter profondément les intérêts des entreprises américaines. Là réside d'ailleurs l'intérêt de la présente étude. Dans la mesure où le texte prétend s'appliquer à toutes les entreprises, même établies en dehors de l'Union européenne, qui offrent des biens et des services à des personnes résidant dans l'Union ou qui observent les comportements de ces dernières[38], il s'imposera aussi bien aux entreprises américaines, y compris ces géants de l'Internet

---

Cette loi, qui est venue transposée la directive du 24 octobre 1995 (évoquée ci-dessous), a eu une incidence limitée sur le droit français, tout en renforçant un certain nombre de garanties : v. J. Frayssinet, « La directive du 24 octobre 1995 relative à la protection des personnes physiques… », Cahiers Lamy, mars 1996 (K), p. 1 et s. ; N. Mallet-Poujol in Lamy Droit du numérique, édition 2012, Lamy, Paris, 2012 (mises à jour Lamyline reflex), n° 558-560.

34 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, JO L 281 du 23.11.1995, p. 31–50.- V. aussi : 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), JO L 201 du 31.7.2002, p. 37–47 (modifiée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006, JO L 105 du 13.4.2006, p. 54–63 et par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, JO L 337 du 18.12.2009, p. 11–36).

35 Charte des droits fondamentaux de l'Union européenne, 2010/C 83/02, art. 8.- Protection des données à caractère personnel : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant.— 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.— 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».- V. aussi Traité sur le fonctionnement de l'Union européenne (TFUE), art. 16, § 1 : « Toute personne a droit à la protection des données à caractère personnel la concernant ».

36 V. toutefois, E.L. Carter, « Argentina's Right to be Forgotten », 27 Emory Int'l L.Rev. 23 (2013).

37 Commission européenne, Proposition de règlement du Parlement européen et du Conseil 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, COM(2012) 11 final, 2012/0011 (COD), Bruxelles, 25.1.2012.

38 Cf. Proposition de règlement du Parlement européen et du Conseil 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, art. 3 (champ

que sont *Google et Facebook* qui, jusqu'à présent, ont souvent traité avec légèreté les dispositifs européens de protection des données[39]. Or, compte tenu de l'importance de ces entreprises, dont les services sont souvent à l'origine même des réflexions actuelles sur le droit à l'oubli, il faut pouvoir anticiper leur possible réaction face à un nouvel instrument européen et mesurer, ce faisant, le degré d'effectivité attendu d'une législation sur le droit à l'oubli[40].

6. Avec l'adoption de la Proposition de règlement du Parlement européen et du Conseil 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[41], le « droit à l'oubli numérique » deviendrait un « droit à l'effacement ». Selon l'article 17, § 1, de la Proposition, la personne concernée aurait « le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données [...] » pour l'un des motifs suivants : « a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées » ; « b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données » ; « c) la personne

---

d'application territorial) et art. 6, § 3.- Cf. Ch. Kuner, « The European Commission's Proposed Data Protection Regulation : A Copernican Revolution in European Data Protection Law », Pricacy & Security Law Report, 11 PVLR 06, 02/06/2012, spéc. p. 3-4 (qui pointe notamment quelques contradictions) ; M. Fazlioglu, « Forget me not : the clash of the right to be forgotten and freedom of expression on the Internet », IDPL 2013, p. 1 et s., spéc. p. 3-5 (qui souligne la difficulté d'identifier le responsable du traitement, le problème du maintien des informations sur des serveurs hors ligne et celui des tiers qui n'ont pas le statut de responsable du traitement ; v. aussi : N. Jääskinen, « Conclusions de l'avocat général » sur CJUE, Google Spain SL Google Inc. c/ Agencia Española de Protección de Datos (AEPD), aff. C-131/12, 25 juin 2013) ; V. Reding, « The European data protection framework for the twenty-first century », IDPL 2012, Vol. 2, No. 3, p. 119 et s., spéc. p. 127.

39 Concernant Google, cf. Article 29 Data Protection Working Party (G29), Letter adressed to Google by the Article 29 Group Brussels, 16.10.2012 (et Annexe : Recommandations du G29 sur les règles de confidentialité de Google http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/GOOGLE_PRIVACY_POLICY-RECOMMENDATIONS-FINAL-FR.pdf). S'agissant de Facebook, cf. Data Protection Commissioner, Facebook Ireland Ltd, Report of Re-Audit, 21 September 2012, http://dataprotection.ie/docs/Facebook_Audit_Review_Report/1232.htm ; G29, Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN WP 192, 22 March 2012. V. aussi la lettre adressée par le ministre allemand à la protection des consommateurs au fondateur de Facebook, Mark Zuckerberg (« David and Goliath ; Data protection in Germany », The Economist (US). 395.8677 (Apr. 10, 2010): p28EU).

40 Espace sans territoire ni frontière, le Cyberespace remet en cause les solutions traditionnelles du droit international privé. Il invite ainsi à réfléchir à des solutions globales, qui prendraient appui sur les textes internationaux : v., par ex., 31e Conférence internationale des commissaires à la protection des données et de la vie privée, Résolution sur des normes internationales sur la vie privée, Madrid, 4,5 et 6 nov. 2009 ; 32e Conférence mondiale des commissaires à la protection des données et de la vie privée, Projet de 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, Jérusalem, 27-29 oct. 2010 ; F. La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.- Summary of cases transmitted to Governments and replies received, United Nations, General Assembly, 27 May 2011, A/HCR/17/27/Add.1. Et plus largement sur cette thématique de l'application de la loi dans l'espace, cf. S.C. Bennett, « The "Right to Be Forgotten" : Reconciling EU and US Perspectives », 30 Berkeley J. Int'l L. 161 (2012), spéc. p. 181-192 ; sous l'angle des flux transfrontières de données : R.H. Weber, « Transborder data transfers : concepts, regulatory approaches and new initiatives », IDPL 2013, Vol. 3, No. 2, p. 117 et s.

41 Précitée.

enfin, « d) le traitement des données n'est pas conforme au présent règlement pour d'autres motifs ». On trouverait ici mieux exprimé ce qui est identifié de longue date comme exprimant un droit à l'oubli dans le domaine de la protection des données personnelles[42] : doit ainsi être limitée dans le temps la conservation des informations sous forme nominative[43] ; mais le texte va plus loin en ajoutant, au-delà du droit d'opposition[44], un cas de retrait du consentement permettant d'obtenir l'effacement en dehors des hypothèses de données inexactes, périmées ou illégitimes[45] – et l'effet du retrait du consentement est désormais rétroactif[46]. Le § 2 du même article ajoute que, lorsque le responsable du traitement a rendu publiques les données à caractère personnel, il doit prendre toutes les mesures raisonnables, y compris techniques, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous les liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci[47]. Dans la proposition de loi du Sénat, aujourd'hui caduque, visant à mieux garantir le droit à la vie privée à l'heure du numérique[48], telle qu'adoptée en première lecture le 23 mai 2010, il était également prévu de modifier la loi n° 78-17 du 6 janvier 1978 de manière à ce qu'il soit précisé que « [d]ès la collecte de données à caractère personnel, le responsable du traitement ou son représentant : — Informe [...] la personne concernée [...] : [...] 3° Des critères déterminant la durée de conservation des

---

42 À propos de la L. n° 78-17 du 6 janvier 1978, v. H. Maisl, « La maîtrise d'une interdépendance », JCP G 1978, I, n° 2891 (cité supra, note (28)). Au sujet des Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel (1980), v. M.D. Kirby, « Transborder Data Flows and the "Basic Rules" of Data Privacy », 27 Stan.J.Int'l L. 62 (1980) qui proposait un principe de limitation dans le temps que l'on trouvait dans une première version des Lignes directrices de l'OCDE : « les données personnelles sous une forme qui permet l'identification du sujet devraient, une fois leur finalité dépassée, être détruites, archivées ou désidentifiées ».

43 V. aussi Lamy droit du numérique.- Informatique, Multimédia, Réseaux, Internet, Éditions Lamy, Paris, 2012, n° 608.

44 L'article 6, qui définit le périmètre des traitements licites, vise tout d'abord l'hypothèse de la personne concernée qui a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques (§ 1, a)). Il faut donc comprendre que, une fois ce consentement retiré, l'effacement devient de droit, puisqu'aucune autre condition n'est exigée. Il existe toutefois des exceptions, prévues par le § 3, dont la liberté d'expression. Le c) du § 1 de l'article prévoit ensuite l'hypothèse de l'exercice du droit d'opposition. L'article 19, § 1 permet à la personne concernée « de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à ce que des données à caractère personnel fassent l'objet d'un traitement fondé sur l'article 6, paragraphe 1, points d), e) et f) ». Mais la disposition ajoute que ce droit d'opposition – qui fait obstacle à ce que le responsable du traitement utilise ou traite les données à caractère personnel concernées (art. 19, § 3) – peut être tenu en échec si le responsable du traitement établit « l'existence de raisons impérieuses et légitimes justifiant le traitement, qui priment les intérêts ou les libertés et droits fondamentaux de la personne concernée ».- Cf., Ch. Kuner, art. préc., p. 6 ; M. Fazlioglu, op. cit., spéc. p. 2 ; V. Reding, art. préc., p. 125.

45 V. aussi Proposition de règlement du Parlement européen et du Conseil 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, cons. 53 et 54.

46 V. aussi, J. Ausloos, « The "Right to be Forgotten" — Worth remembering », C.L.S.Rev. 28 (2012), 143-152, spéc. p. 149-150 ; C. de Terwangne, « Internet Privacy and the Right to Be Forgotten/Right to Oblivion », IDP Número 13 (Febrero 2012), p. 109-121, spéc. p. 118.

47 Sur les limites de cette disposition, v. G29, Avis 01/2012 sur les propositions de réforme de la protection des données, 00530/12/FR, WP 191, 23.03.2012, p. 15 ; M. Fazlioglu, art. préc., spéc. p. 3-4.

48 Proposition de loi, n° 93, présentée devant le Sénat, par Yves Détraigne et Anne-Marie Escoffier, le 6 novembre 2009 (enregistrée à la Présidence du Sénat le 6 nov. 2009).

données à caractère personnel ». Le texte instaurait également un véritable de droit suppression à l'article 8, I : « Lorsque des données à caractère personnel ont été traitées, toute personne physique justifiant de son identité a le droit, pour des motifs légitimes, d'exiger, sans frais, leur suppression auprès du responsable du traitement »[49]. Dans son rapport d'activité pour l'année 2012 la CNIL insiste pareillement sur la nécessité « d'offrir aux utilisateurs des fonctionnalités leur permettant de définir une date de "péremption" de leurs publications ou de gérer leurs propres publications en leur offrant directement la possibilité de les modifier ou de les supprimer ». La Commission remarque également que « l'effectivité du droit à l'oubli devrait être complétée par une obligation de juridique de déréférencement à la charge des moteurs de recherche »[50].

Meilleur respect de la durée de conservation, spécification d'une « date de péremption », droit de suppression pour motif légitime, droit au déréférencement, tous ces mécanismes donneraient chair au droit à l'oubli numérique[51]. Ce dernier vaudrait pour les « traces »[52] laissées à son insu par

---

49 V. CyberLex, Contribution dans le cadre des travaux sur le droit à l'oubli numérique, « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? », Paris, 2012, p. 44.

50 CNIL, 33e Rapport d'activité, La Documentation française, Paris, 2012, p. 83-84

51 V. aussi la Charte sur la publicité ciblée et la protection des internautes, du 30 sept. 2010 (cf. spéc. recommandation n° 5 pour le « droit à l'oubli » des cookies, qui préconise une durée moyenne de 60 jours) et la Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche, du 13 oct. 2010 (cf. spéc. pt. 2.2, 3.2, 3.3, 3.4, 5), deux textes initiés par le secrétariat d'État chargé de la prospective et du développement de l'économie numérique.- Sur ces deux chartes, cf. C. Thiérache, « Le droit à l'oubli numérique : un essai qui reste à transformer », RLDI 2011, n° 67, 2188, p. 6 et s.

52 Les « traces » concernent principalement les données de navigation sur Internet laissées par l'internaute par le biais des témoins de connexion (« cookies ») et des pages restées dans le répertoire « cache » du navigateur. Sont également visés le nom d'hôte (« hostname »), la configuration technique de l'ordinateur, l'adresse IP, le nom du fournisseur d'accès, le système d'exploitation utilisé ou bien encore la provenance de la navigation ayant conduit jusqu'au site visité (cf. Cyberlex, op. cit., p. 50). Deux types de traces suscitent des difficultés particulières : l'adresse IP et les témoins de connexion. L'adresse IP, qui est le numéro qui identifie tout matériel informatique connecté à Internet, permet la localisation de l'internaute, un peu à la manière d'une adresse postale. L'adresse IP est toutefois renouvelée de manière aléatoire à chaque connexion (sauf pour les entreprises et les institutions publiques), et il faut recourir aux fournisseurs d'accès à Internet, qui disposent des fichiers de connexion (« logs »), pour remonter à un ordinateur unique (en fonction de l'adresse IP et de l'heure de connexion). Il s'agit pour la Cour de Justice d'une donnée personnelle : CJUE, 24 nov. 2011, Scarlet Extended, C-70/10, n° 51, Gaz. Pal., 16 févr. 2012, n° 47, note L. Marino, Comm. com. électr. 2012, comm. n° 1, note A. Neri ; v. aussi « Dossier spécial », in RLDI 2012/78, n° 2611 et s. – position partagée par le Groupe de « l'article 29 » (G29, Avis 4/2007 sur le concept de données à caractère personnel, 01248/07/FR, WR 136, 20.06.2007). La jurisprudence française est partagée (cf. Lamy Droit du Numérique, Guide Pratique, Lamy, Paris, 2012, n° 4452 ; et v. Cons. const., 10 juin 2009, déc. n° 2009-580 DC, JORF 13 juin 2009, RLDI 2009/51, n° 1701, note C. Simon). Les témoins de connexion, quant à eux, sont des paquets de données envoyés par le serveur web au navigateur Internet de l'utilisateur. Lorsqu'ils sont installés par le serveur qui héberge la page visité, on parle de « cookies primaires » ou « première partie ». Assez souvent, une page contient d'autres objets ou des publicités qui portent un nom de domaine différent. En affichant la page principale, le navigateur télécharge l'ensemble et peut installer ces cookies venant de serveurs différents, qu'on appelle alors « cookies tiers » ou « tierce partie ». L'intérêt d'un cookie est avant tout de faciliter la navigation. Mais ces témoins de connexion permettent également de dresser des profils socio-culturels, des listes de centres d'intérêts et de préférences de consommation. En cela, et tout comme l'adresse IP, les cookies permettent de pratiquer la publicité dite « comportementale » qui découle d'une analyse des comportements de navigation et des préférences inférées (v. M. Peyrat, CNIL, La publicité ciblée en ligne, Paris, 5 févr. 2009 ; CyberLex, op. cit., p. 60).

l'internaute[53], ainsi que pour les informations diffusées sur les réseaux sociaux[54]. Le droit européen assurerait ainsi mieux la protection de ce qu'il est convenu d'appeler la *vie privée informationnelle*, c'est-à-dire la maîtrise dont bénéficient les sujets de droit sur leurs informations personnelles, comme *précondition* d'une vie autonome[55]. L'enjeu n'est pas l'intimité, mais directement *l'identité et l'autonomie*, c'est-à-dire « le droit à l'autodétermination informationnelle » (*Recht auf informationelle Selbstbestimmung*) pour reprendre la terminologie allemande[56]. La nature de l'information, en tant que telle (privée ou publique, sensible ou anodine), se trouve placée au second plan ; car « le danger inhérent aux traitements de données à caractère personnel réside davantage dans les finalités qu'ils poursuivent que dans la nature des données qui en font l'objet

53 Ces traces ont une grande valeur économique qui devrait s'accroître encore avec l'avènement du Big Data (F.H. Cate, V. Mayer-Schönberger, « Notice and consent in a world of Big Data », IDPL 2013, Vol. 3, No. 2, p. 67 et s.). Il est fondamental que les internautes sachent quelles sont les informations détenues et qui les traite, que la durée de conservation en soit limitée et que l'effacement en soit possible.

54 Il n'est pas certain que les affaires emblématiques du droit à l'oubli, telles celle de Stacy Snyder (cf. V. Mayer-Schönberger, Delete.- Virtue of Forgetting in the Digital Age, op. cit., p. 1-2.- V. Snyder v. Millersville University et al., (mem.)(Dec. 3, 2008) http://www.paed.uscourts.gov/documents/opinions/08d1410p.pdf) ou celles de ces salariés licenciés pour avoir dénigré leur employeur sur leur page Facebook (comp. Rouen, ch. soc., 15 nov. 2011, JurisData n° 2011-028442, Comm. com. électr. 2012, comm. 103, obs. E. A. Caprioli et Cons. prud'h. Boulogne-Billancourt, 19 nov. 2010, JurisData n° 2010-021303, RLDI déc. 2010/66, n° 2177, obs. L.C., Semaine Sociale Lamy 2010, n° 1470, note J.-E. Ray, RLDI janv. 2011/67, n° 2208, note J. Le Clainche ; Besançon, 15 nov. 2011, JurisData n° 2011-031655, Comm. com. électr. 2012, comm. 44, obs. E. Caprioli ; Lyon, ch. soc., 22 nov. 2012, JurisData n° 2012-027024, Comm. com. électr. 2013, comm. 61, obs. E. A. Caprioli), soient propres à éclairer le débat sur la maîtrise des données sur les réseaux sociaux. Il n'est véritablement que deux questions, en plus de celle qui relève de la problématique plus générale des « traces » (v. supra, notes précédentes). La première est celle de la perte de maîtrise : par le jeu de politiques de confidentialité complexes (dont les services de réseautage social – SRS – ont le secret), une information devient très largement accessible et indexé contre le gré de l'utilisateur du réseau social (cf. G29, Avis 5/29 sur les réseaux sociaux en ligne, 12 juin 2009, 01189/09/FR, WP 163 p. 7 : les SRS devraient mettre « en place des paramètres par défaut respectueux de la vie privée, qui permettent aux utilisateurs d'accepter librement et spécifiquement que des personnes autres que leurs contacts choisis accèdent à leur profil, afin de réduire le risque d'un traitement non autorisé »). La seconde question (qui prolonge la première) est celle de la volonté de maîtrise : l'utilisateur d'un réseau social met à jour certaines informations, supprime son compte ou cesse simplement d'utiliser le service de réseautage social ; en ce cas, l'oubli doit être possible, car, comme le relevait Alex Türk, 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 » (A. Türk in CNIL, 30e Rapport d'activité, La Documentation française, Paris, 2009, p. 29). V. les solutions préconisées par le G29 (G29, Avis 5/2009, op. cit., p. 9, 11-12), à mettre en perspective avec les durées de conservation prévues par l'article 6, II, de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), ainsi que dans l'article 1er, 1° et 2, et l'article 3 du décret n° 2011-219 du 25 févr. 2011 (JORF n° 0050 du 1er mars 2011).

55 La maîtrise n'est pas une fin en soi ; elle n'est qu'instrumentale. Sur cette distinction fondamentale : cf. A. Rouvroy, Y. Poullet, « The Right to Self-Determination and the Value of Self-Development : Reassessing the Importance of Privacy for Democracy », in S. Gutwirth et al. (ed.), Reinventing Data Protection ?, Springer, Dordrecht, London, 2009, p. 45, spéc. p. 51.

56 Cour Constitutionnelle fédérale allemande, 15 déc. 1983, EuGRZ 1983, p. 171 et s. ; Droit de l'informatique et des télécoms 1985, n° 4, p. 8-16, note H. Burkert, Human Rights Law Journal 1984, Vol. 5, No. 1, p. 67 et s. Pour la Cour Constitutionnelle, « le droit à l'autodétermination en matière d'information » fait partie intégrante des droits généraux de la personne humaine : « La valeur et la dignité de la personne humaine agissant librement comme membre d'une société libre sont les principes essentiels de la loi fondamentale » (H. Burkert, op. cit., p. 8). L'enjeu reste le libre épanouissement de la personnalité (Loi Fondamentale, art. 2.1).

»[57]. Pour limiter les effets potentiellement dangereux de ces traitements de données – qui permettent de reconstituer l'identité, d'anticiper sur le comportement d'une personne[58] –, on invoque souvent, comme prolongement de l'aptitude reconnue à chacun de déterminer quand et dans quelles limites des informations personnelles doivent être divulguées, un droit à l'oubli, en tant que *droit à l'effacement sur demande du sujet, au-delà d'un certain délai ou dès lors que la finalité ayant justifié le récolement ait atteinte*[59] ; pour le moins, *un droit au contrôle de l'information*[60].

7. Les revendications en faveur d'un droit à l'oubli numérique se sont également manifestées sur un autre front : celui du droit à la *vie privée personnelle*. Le problème est ancien, puisqu'à l'origine des premières évocations du droit à l'oubli. Il s'agit d'informations préjudiciables à la personne et, parfois, d'informations d'ordre judiciaire qui, à une époque donnée, ont été livrées à la connaissance du public, par la personne elle-même ou par autrui en vertu d'une autorisation de la loi ou du contrat, et qui font l'objet quelques années plus tard d'une redivulgation (republication)[61]. Avec l'apparition de l'Internet, le problème est devenu beaucoup plus sensible du fait de la persistance en ligne de l'information et des modalités d'accès à l'information qu'offrent les moteurs de recherche. Les hypothèses concrètes de redivulgations dommageables sont variables[62] : évocation d'un passé peu glorieux que le temps semblait avoir enfoui et dont la résurrection vient compromettre la réhabilitation de la personne ou porte atteinte à l'une de ses libertés[63] ; relation, par un journal, de la mauvaise santé financière d'un chanteur, elle-même reconnue dans un récit autobiographique[64]. En s'ajoutant, la persistance de

---

57 M.-H. Boulanger, C. de Terwangne, Th. Léonard, « La protection de la vie privée à l'égard des traitements de données à caractère personnel – La loi du 8 déc. 1992 », J.T. 1993, p. 369, spéc. p. 377. V. aussi : O. de Schutter, note ss. CEDH, 4 mai 2000, Rotaru c/ Roumanie, requête n° 28341/95, RTDH 2001, p. 137 et s., spéc. p. 166 : « [I]l importe peu [...] que l'individu ait exprimé publiquement telle opinion politique, ou pratiqué ouvertement tel culte ; c'est le fait du traitement, en tant que tel, et en raison de la suspicion qui entoure la collecte, l'enregistrement, la conservation et l'utilisation de telles données à caractère personnel, contre lequel il est protégé » ; v. aussi : D. Solove, « A Taxonomy of Privacy », 54 U. Pa. L. Rev. 477 (2006), p. 507.

58 V., entre autres références, Ch. Conley, « The Right to Delete », AAAI Spring Symposium Series, North America, 2010, p. 53 et s., spéc. p. 53 ; J. Ausloos, « The "Right to be Forgotten" — Worth remembering », op. cit., spéc. p. 144-145.

59 Sur les questions que soulève, abstraitement, un droit à l'effacement, cf. Ch. Conley, op. cit., p. 55-56 ; sur les limites techniques, cf. European Network and Information Security Agency (enisa), The right to be forgotten – between expectations and practice, Heraklion, 2011 ; J. Le Clainche, « L'adaptation du "droit à l'oubli" au contexte numérique », R.E.D.C. 2012/1, p. 39 et s.

60 A. Rouvroy, « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information », in S. Lacour (dir.), La sécurité de l'individu numérisé.- Réflexions prospectives et internationales, L'Harmattan, Paris, 2009, p. 249-278, spéc. p. 252 : « Nous voulons soutenir que l'une des conditions nécessaires à l'épanouissement de l'autonomie individuelle est, pour l'individu, la possibilité d'envisager son existence non pas comme la confirmation ou la répétition de ses propres traces, mais comme la possibilité de changer de route, d'explorer des modes de vie et façons d'être nouveaux, en un mot, d'aller là où on ne l'entend pas, voire même là où il ne s'attend pas lui-même ».- V. aussi les remarques de P.A. Bernal, « A Right to Delete ? », European Journal of Law and Technology, Vol. 2, No. 2 (2011), spéc. § 3.1, 3.2 et 3.6.- Et v. infra, conclusion, n° 87, les remarques sur la notion de contrôle.

61 V. les affaires classiques citées supra, n° 4.

62 Il peut s'agir d'une diffamation, si les faits redivulgués, ayant autrefois entraîné une condamnation pénale, ont depuis lors été amnistiés : TGI Paris, 17e ch., 12 mai 2010, Patrick D. c/ Sté Nice Matin et a., RLDI 2010, n° 62.

63 Comp. Civ. 1re, 20 nov. 1990, Bull. civ. 1990, I, n° 256, JCP G 1992, II, 21 908, note J. Ravanas.

64 CEDH, 23 juill. 2009, Affaire Hachette Filipacchi Associés (« Ici Paris ») c/ France, requête n° 12268/03.

l'information en ligne aggrave le phénomène de republication en la maintenant virtuellement accessible de manière illimitée.

Mais la persistance en ligne de l'information constitue, *par elle-même*, une nouvelle difficulté. Le problème se pose essentiellement pour la presse en ligne[65], qui est bien souvent le « prolongement électronique de médias papier »[66]. En matière judiciaire, le journal électronique devient un immense traitement automatisé de données[67] comparable à un « casier judiciaire virtuel »[68] qui, d'abord, bloque toute capacité d'oubli, ensuite modifie considérablement la « temporalité informationelle »[69]. L'oubli devient, en effet, difficile, sinon impossible, car « il suffit qu'un justiciable ait été cité une fois dans un journal pour que la numérisation et la mise sur internet de ce journal le désignent à jamais et rappellent les circonstances dans lesquelles la personne concernée a eu à faire avec la justice »[70]. Surtout, l'information, à laquelle il n'est plus nécessairement accédé par la page d'accueil du journal (qui contient normalement l'information la plus récente), se trouve sortie de son « ordonnancement chronologique »[71] à la faveur des résultats de l'algorithme des moteurs de recherche ou des jeux de liens hypertextes, ou parce que l'épilogue éventuellement favorable n'est pas précisé[72]. D'aucuns estimeront que, la révélation ayant eu lieu licitement, on ne saurait sanctionner la redivulgation[73]. C'est aujourd'hui la position

---

65 Mais pas seulement : Viktor Mayer-Schönberger a mentionné le cas du psychiatre et psychanalyste canadien, Andrew Feldmàr. Alors qu'il s'apprête à traverser par la route la frontière entre le Canada et les États-Unis, il se voit refuser l'accès au territoire étasunien pour un article publié en 2001 dans une revue scientifique. C'est que le garde-frontière, qui avait retrouvé ledit article en interrogeant le mot « Feldmàr » sur un moteur de recherche, s'était rendu compte que Feldmàr y relatait la prise de LSD dans les années 1960 (V. Mayer-Schönberger, Delete.- Virtue of Forgetting in the Digital Age, op. cit., p. 3-4).- V. aussi : TGI, Paris, réf., 15 févr. 2012, Diana Z. c/ Google, Comm. com. électr. 2012, comm. 54, obs. A. Lepage ; TGI Montpellier, ord. réf., 28 oct. 2010, C. c/ Google France et Google Inc., Comm. com. électr. 2011, comm. 47, obs. A. Lepage.

66 N. Mallet-Poujol, « Presse en ligne et droit à l'oubli numérique : nouvelles responsabilités », in É. Vergès (dir.), Droit, sciences et techniques : quelles responsabilités, Litec, Paris, 2011, p. 283 et s., spéc. p. 297.

67 N. Mallet-Poujol, op. cit., loc. cit.

68 CyberLex, Rapport précité, p. 103 et s.

69 N. Mallet-Poujol, op. cit., p. 304.

70 CNIL, Délib. n° 01-057, 29 nov. 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence.

71 N. Mallet-Poujol, op. cit., p. 304, CyberLex, op. cit., p. 105.

72 Cyberlex, op. cit., p. 105 : « À titre d'exemple, une personne condamnée en première instance dans le cadre d'une procédure pénale mais relaxée en appel peut éventuellement être toujours citée comme délinquante dans des articles anciens, encore accessibles et éventuellement indexés par un moteur de recherche ».

73 Selon l'analyse traditionnelle, s'il n'y a normalement pas d'atteinte à la vie privée en cas d'autorisation personnelle à la divulgation par le titulaire du droit (J.-Ch. Saint-Pau, « Jouissance des droits civils.- Droit au respect de la vie privée.- Régime.- Atteinte légitime à la vie privée », J.-Cl. Civil Code, art. 9, Fasc. 15, n° 8 et s.), chaque autorisation doit néanmoins être spéciale (« la personne a seule le droit de fixer les limites de ce qui peut être publié ou non sur sa vie intime, en même temps que les circonstances et les conditions dans lesquelles ces publications peuvent intervenir » : Paris, 13 févr. 1971, JCP G 1971, II, 16774, note R. Lindon). Il s'ensuit que toute redivulgation doit normalement faire l'objet d'une nouvelle autorisation (v. les exemples donnés par J.-Ch. Saint-Pau, Fasc. préc., n° 25 et s.). Cette jurisprudence classique paraît toutefois battue en brèche par la Cour de cassation qui énonce désormais « qu'il n'y a pas atteinte à la vie privée lorsque les prétendues révélations ne sont que la relation de faits publics ou ne présentent qu'un caractère anodin » (Civ. 1re, 3 avr. 2002, n° 99-19.852, JurisData n° 2002-013788, D. 2002, p. 3164, note C. Bigot ; D. 2003, p. 1543, obs. Caron, JCP G 2003, I, 126, n° 11, obs. Tricoire, Gaz. Pal. 2003, 1040, note

de la Cour de cassation qui, à propos de la maîtresse d'un ancien collaborateur entendant s'opposer à la publication d'un ouvrage sur cette période honnie, notait que « les faits touchant à la vie privée d'une personne ayant été livrés en leur temps à la connaissance du public par des comptes rendus de débats judiciaires [...], l'intéressé ne pouvant se prévaloir d'un droit à l'oubli pour empêcher qu'il en soit de nouveau fait état »[74]. Mais on pourrait aussi admettre qu'un fait intime (personnel), un temps devenu public, retourne dans la sphère privée au nom du droit à l'oubli[75]. À l'instar de cette décision souvent citée du tribunal de grande instance de Paris, rendue dans le cadre de la presse traditionnelle, on devrait reconnaître que « toute personne qui a été mêlée à des événements publics peut, le temps passant, revendiquer le droit à l'oubli » ; et que, sauf exception tirée d'un événement historique ou d'actualité, « ce droit à l'oubli qui s'impose à tous, y compris aux journalistes, doit également profiter à tous, y compris aux condamnés qui ont payé leur dette à la société et tente de se réinsérer »[76]. Là encore, des remèdes ont été proposés[77], dont l'un d'eux consisterait dans une formalisation de ce droit à l'oubli évoqué par le tribunal[78].

8. Le cadre de comparaison est d'une remarquable complexité. Et pourtant, il lui manque encore la prise en compte des droits et libertés antagonistes, comme la liberté d'expression, la liberté de la presse[79], la liberté du commerce et de l'industrie, la protection de la sécurité publique

---

Toucas et Juillard, Comm. com. électr. 2002, comm. 158, note Lepage ; Dr. et patrimoine 2003, p. 115, obs. Loiseau ; Civ. 1re, 23 avr. 2003, D. 2003, p. 1854, note C. Bigot).- C'est aussi la position de la CEDH, v. infra, note (72).

74 Civ. 1re, 20 nov. 1990, préc.- V. aussi : V. aussi CEDH, 23 juill. 2009, Affaire Hachette Filipacchi Associés (« Ici Paris ») c/ France, requête n° 12268/03, Comm. com. électr. 2009, comm. n° 93, obs. A. Lepage : « les informations, une fois portées à la connaissance du public par l'intéressé lui-même, cessent d'être secrètes et deviennent librement disponibles ».

75 En ce sens, Ch. Caron, « À propos du conflit entre les œuvres de fiction et la vie privée », D. 2003, p. 1715 ; A. Marais, art. préc., n° 12.

76 TGI, 20 avril 1983, JCP G 1983, II, 204 034, obs. R. Lindon.- V. aussi la position de la CEDH qui reconnaît que « le passage du temps doit nécessairement être pris en compte » : CEDH, 18 mai 2004, Éditions Plon c/ France, requête n° 58148/00, § 53, D. 2005, p. 1838, note A. Guedj, D. 2005, somm. p. 2539, obs. N. Fricéro, RTD civ. 2004, p. 483, obs. J. Hauser.- V. aussi, en droit italien : Cass. ital., 9 avr. 1998, n° 3679, For. it. 1998, I, 1834 : « De manière plus analytique, l'arrêt d'appel a rappelé que, en raison du temps long qui s'est écoulé entre les deux publications, l'auteur de la seconde [publication] avait l'obligation de compenser "les effets libérateurs du passage d'une longue période temps", de vérifier l'existence possible de nouveaux rapports ou de nouvelles actions en justice à l'encontre de Rendo ». La Cour de cassation note un peu plus loin : « Se fait jour, cependant, un nouvel aspect de la vie privée qui, récemment, a également été défini comme droit à l'oubli, entendu comme le juste intérêt, pour chaque personne, de ne pas demeurer exposée de manière indéterminée à des dommages ultérieurs causés à son honneur et sa réputation du fait de la republication d'une nouvelle légitimement dilvulguée par le passé » (v. aussi : G. Pino, « The Right to Personal Identity in Italian Private Law : Constitutional Interpretation and Judge-Made Rights », in M. Van Hoecke, F. Ost (ed.), The Harmonization of Private Law in Europe, Hart Publishing, Oxford, 2000, p. 225-237 ; G. Finocchiaro, « La memoria della rete e il diritto all'oblio », op. cit., p. 397).

77 On se contente de renvoyer à l'article très complet de N. Mallet-Poujol, op. cit., spéc. p. 299 et s.

78 Il s'agirait notamment de la désindexation des articles litigieux : TGI, Paris, 25 juin 2009, Légipresse nov. 2009, n° 266, III, p. 215 et s., note N. Mallet-Poujol ; v. aussi, récemment, dans l'affaire dite M. Mosley (évoquée ailleurs dans cet ouvrage, page 134) : TGI Paris, 6 nov. 2013, Max Mosley/Google.- V. aussi l'affaire du chirurgien espagnol, Guidotti Russo, évoqué dans cet ouvrage par A. Rallo, p.240 ******

79 V. notamment S. Proust, « Le projet de règlement européen sur le droit à l'oubli ou l'enterrement programmé de la loi de 1881 sur la liberté de la presse », Légipresse n° 304, avr. 2013, p. 211 et s. ; M. Fazlioglu, art. préc., p. 5-7 ; J. Rosen, « The Right to be Forgotten », 64 Stan. L. Rev. 88 (2012), p. 90-92.

ou les droits de l'Histoire[80]. On y viendra directement avec l'étude du droit américain en soulignant, le cas échéant, les différences[81]. En tout état de cause, cette complexité n'est pas seule due à la variété des situations, la haute technicité des questions et l'ampleur des interactions individuelles. Il faut bien reconnaître que la question du fondement possible du droit à l'oubli ne laisse pas de susciter la perplexité de l'interprète. Dans toutes les hypothèses où l'intimité (le fait privé ou personnel) n'est pas *directement* en jeu, seulement la maîtrise de l'information – « vie privée informationnelle » – le droit à l'oubli oblique vers la protection des données personnelles et entend plutôt préserver l'identité personnelle et la liberté – liberté au sens de participation à la sphère publique (la *vita activa*)[82], « *freedom* » et non pas « *liberty* »[83]. À l'inverse, lorsque c'est l'intimité, la vie personnelle qui est menacée, le droit à l'oubli s'ente sur le droit à la vie privée originel – « vie privée personnelle » – dans sa version *érémitique, corporelle, sensorielle ou domiciliaire*[84]. Les finalités paraissent alors différentes : au-delà de l'intimité, c'est le secret, l'anonymat ou la solitude que l'on cherche à préserver ; peut-être aussi l'autonomie individuelle et l'indépendance morale. Doit-on alors encore parler de vie privée, et donc d'*un* droit à l'oubli ? Les ponts ne sont-ils pas définitivement coupés, comme le donne à penser la Charte des droits fondamentaux de l'Union européenne qui traite séparément de la vie privée et de la protection des données ?[85]

Rien n'est moins sûr. Les deux fondements peuvent parfois se superposer[86], d'abord parce qu'ils ont tous deux une dimension instrumentale[87] et partant des périmètres d'action communs[88] ;

---

80 Cf. les observations nuancées de P.A. Bernal, « A Right to Delete ? », op. cit., § 3.2.

81 V. infra, n° 24 et s.

82 H. Arendt, Condition de l'homme moderne, Calman-Lévy, Paris, 1983, p. 76-77, p. 109.

83 H. Arendt, On Revolution, Penguin Classics, London, 1963, p. 124. Sous ce regard, la vie privée a beaucoup à voir avec la démocratie délibérative, telle qu'on la trouve exprimée chez Rawls et Habermas notamment ; cf. A. Rouvroy, Y. Poullet, op. cit., p. 58 ; P.M. Schwartz, « Beyond Code for Internet Privacy : Cyberspace, Filters, Privacy control, and Fair Information Practice », 2000 Wis. L. Rev. 743, spéc. p. 787 ; v. aussi, sur le risque du conformisme : Ch. Conley, « The Right to Delete », op. cit., p. 54.

84 Encore qu'il se trouve des auteurs pour défendre la dimension sociale de la vie privée personnelle ; cf. not. P. Regan, Legislating Privacy : Technology, Social Values and Public Policy, University of North Carolina Press, Chapel Hill, N.C, 1995, p. 213 : qui considère que la vie privée a une valeur commune (tous les individus attachent une certaine importance à la vie privée et partagent des conceptions communes sur celle-ci), une valeur publique (en ce qu'elle a de l'importance pour le système politique libéral) et une valeur collective (nul ne pouvant bénéficier d'une sphère protégée sans que tous les membres d'une société bénéficient ensemble d'un degré minimum et équivalent de vie privée) ; v. aussi D.J. Solove, Understanding Privacy, Havard University Press, Cambridge, London, 2008, p. 98.

85 Cf. M.L. Ambrose, J. Ausloos, « The Right to Be Forgotten Across the Pond », Journal of Information Policy 3 (2013), 1-23, spéc. p. 2, 14, 15 et s. qui voient dans la Proposition de règlement deux formes de droit à l'oubli (« right to be forgotten ») : un « right to oblivion » (droit à l'oubli) propre à la vie privée personnelle et un « right to erasure » (droit à l'effacement) attaché à la vie privée informationnelle.

86 Cons. const., 10 juin 2009, déc. n° 2009-580 DC, JORF 13 juin 2009, cons. 27 : « l'autorisation donnée à des personnes privées de collecter les données permettant indirectement d'identifier les titulaires de l'accès à des services de communication au public en ligne conduit à la mise en œuvre, par ces personnes privées, d'un traitement de données à caractère personnel relatives à des infractions ; qu'une telle autorisation ne saurait, sans porter une atteinte disproportionnée au droit au respect de la vie privée, avoir d'autres finalités que de permettre aux titulaires du droit d'auteur et de droits voisins d'exercer les recours juridictionnels dont dispose toute personne physique ou morale s'agissant des infractions dont elle a été victime » ; CEDH, 21 janv. 1999, Tsachividis c/ Grèce, requête n° 28802/95, § 43, CEDH, 4 mai 2000, Rotaru c/ Roumanie, requête n° 28341/95, § 43- Comp. TGI, 12 oct. 2009, RLDI 2009/54, n° 1798, note J. Frayssinet.- V. surtout les remarques faites infra, n° 51.

ensuite, et surtout, parce que les situations ne sont jamais nettes au point de se laisser couler dans une seule des catégories en jeu. Tout comme la vie privée, le droit à l'oubli est un concept trop complexe pour être ramené à une essence unique (au-delà de cette valeur sociale et individuelle – la nécessité de l'oubli – qui paraît subsumer les différentes parties, les notions éclatées). Il n'en demeure pas moins que les classes (universaux, catégories génériques) dégagées ci-dessus ont quelque chose à voir entre elles. Il est difficile de dire précisément quoi – on est encore dans le domaine du ressenti[89] (comme lorsqu'on dit : « Celui qui ne sait pas se reposer sur le seuil du moment, oubliant tout le passé, ne saura jamais ce qu'est le bonheur »[90] ; « l'oubli [...] est un si puissant instrument d'adaptation à la réalité parce qu'il détruit peu à peu en nous le passé survivant qui est en constante contradiction avec elle »[91]). Mais ce ressenti est éclairant et doit être exploité. Il renvoie à ce que la philosophie de Wittgenstein appelle « l'air de famille »[92]. Certaines choses, en effet, ne partagent pas de caractéristiques communes, mais n'en sont pas moins reliées entre elles de différentes façons.

9. C'est ce qui doit ressortir de cette étude qu'il faut désormais consacrer entièrement au droit des États-Unis. Pour ce faire, et après un prélude nécessaire consacré à la notion de vie privée aux États-Unis (1), il conviendra d'envisager successivement le droit à l'oubli dans ses rapports avec la vie privée personnelle (2) et la vie privée informationnelle (3).

Section 1- La notion de vie privée aux Etats-Unis

10. Comme le remarquait le Professeur Rigaux, la notion de vie privée n'a pas subi la phase de profonde uniformisation qu'ont connue les concepts apparus à peu près à la même période. La matière est, en effet, « demeurée beaucoup plus dépendante des traditions nationales »[93] et les différences sont restées grandes entre vie privée, « droit au libre épanouissement de la personnalité » (« *das Recht auf die freie Entfaltung seiner Persönlichkeit* ») et *privacy*, alors même que la

87 A. Rouvroy, Y. Poullet, « The Right to Self-Determination and the Value of Self-Development : Reassessing the Importance of Privacy for Democracy », op. cit., p. 50.

88 Sur cette question, v. J. Rochfeld, « Quels sont les liens de la vie privée et de la protection des données à caractère personnel ? », Questions actuelles sur la commercialisation des données à caractère personnel (Entretien avec D. Cohen, R. Perray, J. Rochfeld, A. Soreau), Cah. dr. entr. 2012, entretien 3.

89 D'ailleurs, ainsi qu'on a pu le dire, la vie privée « se sent plus qu'elle ne se définit », J. Velu, R. Ergec, « Convention européenne des droits de l'homme », Rép. prat. dr. belge, n° 652, cité par F. Sudre, « Rapport introductif.- La "construction" par le juge européen du droit au respect de la vie privée », in F. Sudre (dir.), Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme, Bruylant, Bruxelles, 2005, p. 11-33, spéc. p. 11.

90 F. Nietzsche, « Considérations inactuelles » (Deuxième partie), in Œuvres, Gallimard, La Pléiade, Paris, 2002, p. 502.

91 M. Proust, À la recherche du temps perdu. XIII Albertine disparue, Gallimard, Paris, 1925, p. 172.

92 L. Wittgenstein, Le Cahier bleu et le Cahier brun (tr. fr. Goldberg et Sackur), Gallimard, Paris, 1996, p. 57-58 ; idée que nous empruntons à D.J. Solove, Understanding Privacy, op. cit., p. 42 et s. ; D.J. Solove, « A Taxonomy of Privacy », art. préc., p. 485 et s.

93 F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, Bruylant, LGDJ, Bruxelles, Paris, 1990, p. 7.

plupart des systèmes juridiques occidentaux ont pris conscience, à peu près à la même période et sous l'influence des mêmes facteurs[94], de la nécessité d'une protection effective de la vie privée. C'est que, aux États-Unis comme ailleurs, l'histoire politique, économique et sociale a joué un rôle crucial dans la structuration de la notion (I) puis dans l'articulation de la notion avec les droits et libertés concurrents (II).

I- La structuration de la notion

11. L'histoire du développement de la vie privée aux États-Unis est une histoire singulière qui ne doit presque rien au *common law* anglais. C'est la première surprise pour l'observateur qui doit s'attendre à en faire une autre : alors que, comme le remarquait le Doyen Strömholm, c'est aux États-Unis que la question de la protection juridique s'est d'abord posée « avec une particulière acuité »[95], que c'est aux États-Unis aussi qu'ont été diagnostiquées précocement[96] les menaces de l'informatique sur les libertés, le droit américain ne dispose pourtant d'aucun texte général garantissant une large protection de la vie privée. Pour des raisons socio-culturelles complexes, le droit américain n'est jamais parvenu à structurer la notion de vie privée qui est aussi bien restée profondément fragmenté (A). Un regard superficiel pourrait laisser croire que la jurisprudence constitutionnelle est parvenue à réaliser ce qui avait semblé hors de portée du *common law* et du *statute law*. Si le célèbre arrêt *Griswold v. Connecticut* de 1965 (rendu en matière de contraception) a bien permis à la Cour Suprême de découvrir un *right to privacy* constitutionnel cohérent dans les « clairs-obscurs » (« *penumbras* ») du *Bill of Rights*[97], il ne s'agissait alors que la vie privée décisionnelle[98], ce que l'on appelle parfois encore la vie privée-liberté[99]. Aucune unification n'a eu lieu au-delà, que ce soit entre la vie privée décisionnelle et la vie privée informationnelle et personnelle ou bien encore à l'intérieur de ces deux dernières catégories (B).

A-Une notion fragmentée

12. Très pragmatique, le droit américain a répondu à des problèmes divers et a donné naissance, au gré des circonstances, à un corpus complexe de dispositions d'origine diverse qui se superposent aujourd'hui. Ce corpus forme le droit au respect de la vie privée aux États-Unis.

---

94 C'est au cours de la première révolution technologique (1880-1950), celle de la naissance du microphone, du téléphone et de la photographie instantanée, de la constitution de sociétés de masse et l'apparition de moyens de communication de masse, enfin de la prise de conscience du pluralisme des idéologies et des convictions, que la notion de vie privée accède progressivement à la vie juridique (F. Rigaux, op. cit., p. 18-20).

95 Strömholm, in Travaux de l'Association Henri Capitant, Le secret et le droit, Journées libanaises, t. XXV, 1974, note (354), p. 188-189, cité par P. Kayser, La protection de la vie privée par le droit : protection du secret de la vie privée, 3e éd., PUAM, Economica, Aix-en-Provence, Paris, 1995, p. 91.

96 En 1973, avec l'important rapport du United States Department of Health, Education, and Welfare (HEW) ; v. infra, n° 16.

97 Griswold v. Connecticut, 381 US 479 (1965). L'arrêt est évoqué infra, note (176).

98 A.L. Allen, « Constitutional law and privacy », in D. Patterson, A companion to philosophy of law and legal theory, Blackwell, Oxford, 1996, p. 139-155.- V. aussi J. DeCew, V° Privacy, in E. N. Zalta, The Standford Encyclopedia of Philosophy, 2002.

99 F. Sudre, Droit européen et international des droits de l'homme, 10e éd., PUF, Paris, 2011, p. 501.

Il faudra parfois remonter à la naissance même des États-Unis pour saisir la *privacy* américaine dans toute sa subtilité[100]. On peut se contenter pour l'heure d'explorer une période plus proche, la fin du XIX[e] siècle. C'est à cette époque que Samuel Warren et Louis Brandeis[101] rédigent un article majeur, « The Right to Privacy »[102], dont Roscoe Pound a pu dire qu'il n'a fait « rien moins qu'ajouter un chapitre à notre droit »[103]. L'article – qui est aussi un plaidoyer – intervient à un moment charnière. La presse sensationnelle (« *yellow journalism* », « *yellow press* »)[104] connaît un tel succès que, entre 1850 et 1890, le taux de circulation de ces journaux, qui s'emploient « à arracher le toit des résidences privées »[105] selon l'heureuse image de Dickens, augmente de 1 000%[106]. L'autre changement majeur qui s'amorce au même moment est l'avènement de nouvelles technologies qui sont perçues comme autant de menaces pour l'intimité. La photographie, en particulier, se démocratise avec l'arrivée sur le marché d'appareils photo suffisamment compacts et économiques pour toucher un large public. Même si, à l'époque de Warren et Brandeis, les journaux ne publiaient pas même de dessins, les deux juristes ont anticipé les conséquences de ces nouveaux appareils photographiques. Ces circonstances[107] ont contribué à jeter une lumière

---

100 V. infra, n° 17 et s.

101 Ce dernier deviendra juge à la Cour Suprême des États-Unis.

102 S.D. Warren, L.D. Brandeis, « The Right to Privacy », Harvard Law Review, vol. 4 (1890), p. 193-220 (dont on trouvera une traduction proposée par Françoise Michaut dans la revue Clio@Themis : S.D. Warren, L.D. Brandeis, « Le droit à la vie privée (1890) », in Clio@Themis n° 3).

103 A.Th. Mason, Brandeis : A Free Man's Life, The Viking press, New York, 1946, p. 70 (cité par D.J. Solove, P.M. Schwartz, Information Privacy Law, 4th ed., Wolters Kluwer, New York, 2011, p. 10). On a pu également dire qu'il s'agit « de l'article juridique le plus influent jamais écrit » : H. Kalven, Jr., « Privacy in Tort Law — Were Warren and Brandeis Wrong ? », 31 L. & Comtemp. Prons. 326, 327 (1966). L'arrêt Kyllo v. United States, 533 U.S. 27 (2001) s'y réfère à des multiples reprises.

104 En 1833, Benjamin Day lançait un nouveau journal, le Sun, sur le modèle des « penny press newspapers » à Londres (journaux qui se vendaient à un prix dérisoire). Le Sun faisait état des scandales, tels que les querelles familiales, les ivresses publiques, les infractions mineures. En 4 mois, le Sun atteignit un nombre moyen de lecteur de l'ordre de 4 000, soit l'équivalent, à peu de choses près, des quotidiens new-yorkais.

105 Ch. Dickens, American Notes for General Circulation and Pictures from Italy, Chapman & Hall, London, 1913, Chapter VI ; v. aussi Vie et aventures de Martin Chuzzlewit (trad. A.S. Langlois Des Essarts), Vol. 1, Hachette, Paris, 1866, p. 290, les noms fantasques et peu flatteurs dont le romancier anglais affuble les journaux new-yorkais : le New-York-Sewer, le New-York-Stabber, le New-York-Private-Listener, le New-York-Peeper, le New-York-Keyhole-Reporter, New-York-Rowdy-Journal.

106 D. Solove, P.M. Schwartz, op. cit., p. 11.

107 Il ne faut pas négliger l'importance de deux articles publiés en 1890 par E.L. Godkin, un célèbre commentateur social de l'époque (E.L. Godkin, « The Rights of the Citizen : To His Own Reputation », Scribner's Mag (1890) ; « The Right to Privacy », The Nation (Dec. 15, 1890) ; extraits du premier in D. Solove, P. Schwartz, op. cit., p. 11-12). Les idées que partagent Godkin, d'une part, et Warren et Brandeis, de l'autre, sont très nombreuses ; avec une différence toutefois : Godkin ne pensait pas qu'il fût possible de remédier à la situation par une action politique. Il exprimait simplement l'espoir que les comportements changeraient de manière à mieux respecter la vie privée. Telle n'était évidemment pas l'opinion de Warren et Brandeis qui ne croyaient que dans une action directe du droit (v. aussi : D.J. Glancy, « The Invention of the Right to Privacy », 21 Ariz. L. Rev. 1 (1979). On mentionne assez souvent la situation de Warren qui était un riche et puissant avocat de Boston. Il se maria en 1883 avec Mabel Bayard, fille d'un sénateur important du Delaware, et il emménagea dans une maison située à Back Bay, riche quartier de Boston. Les Warrens faisaient partie de l'élite de ville et se retrouvaient ainsi fréquemment dans la Saturday Evening Gazette qui faisait profession de détailler l'intimité de ces personnalités notoires. William Prosser a soutenu que ce qui a conduit Warren à écrire l'article est l'intrusion de journalistes lors de la cérémonie de mariage de sa fille. Mais comme Solove et Schwartz l'ont justement remarqué, en 1890, la fille de Warren n'était âgée que de 10 ans (D. Solove, P.

crue sur les insuffisances du *common law* dans la protection de la *privacy*, que les *remèdes* fussent tirés du droit des contrats ou du droit de propriété[108]. C'est d'ailleurs au constat de ces insuffisances qu'ils proposaient la consécration d'un nouveau droit, le droit à la vie privée (« *right to privacy* »), qu'ils définissaient, reprenant la formule d'un traité sur les *torts* de Thomas Cooley[109], alors juge en chef à la Cour Suprême du Michigan, comme le « droit d'être laissé seul », « le droit d'être laissé tranquille » – « *the right to be let alone* » – en tant que « partie d'un droit plus général à l'intégrité personnelle, le droit à la personnalité » , à « l'inviolabilité de la personnalité ». Quelques mois seulement après la publication de l'article, la Cour Suprême des États-Unis citait ainsi le même passage du traité de Cooley, dans l'affaire *Union Pacific*[110].

13. Dans les années qui ont suivi la publication de l'article, les juges se sont efforcés de répondre à l'appel de Warren et Brandeis en créant des *privacy torts*[111]. Sans doute moins respectueux des précédents que les juges anglais et sensibilisés très tôt à leur pouvoir créateur et leur rôle politique, les juges américains n'en ont pas moins ressenti parfois vivement les limites démocratiques que présentait la création spontanée d'une nouvelle action en responsabilité civile sur le fondement du *common law* (« *common law tort action* ») pour réparer les atteintes à la vie privée (« *privacy invasions* »). Telle fut l'attitude prudente de la *Court of Appeals* de New York dans l'affaire *Roberson v. Rochester Folding Box Co*[112] qui refusa de faire droit à la demande de réparation de l'atteinte à l'image et à la réputation d'une adolescente dont une lithographie la représentant avait servi à illustrer une campagne publicitaire pour une farine. Pour les juges, « [l]es juridictions [...] n'ayant point le pouvoir de légiférer, sont contraintes d'adjuger selon les principes ». Constatant

---

Schwartz, op. cit., p. 12 qui s'appuient sur J.H. Barron, « Warren and Brandeis, The Right to Privacy », 4 Harv. L. Rev. 193 (1890)).

108 Dans l'un et l'autre cas, Warren et Brandeis jugent les solutions peu satisfaisantes. Le droit de propriété, d'utile secours pour la protection des œuvres littéraires et artistiques, est impuissant à intervenir « là où la valeur de la production ne se trouve pas dans le droit de faire des profits issus de la publication » S.D. Warren, L.D. Brandeis, « Le droit à la vie privée (1890) op. cit., spéc. § 10. Car l'intérêt que le sujet de droit veut voir protéger, est « la tranquillité d'esprit ou le soulagement offerts par la capacité à empêcher toute publication » (ibid.). Quant au fondement du contrat, s'ils le jugeaient suffisant dans une société pré-technologique, ils l'estimaient incapable de répondre aux besoins nouveaux : « maintenant que les moyens modernes offrent de multiples occasions de perpétrer de tels dommages sans participation quelconque de la partie lésée, la protection accordée par le droit doit se fonder sur une base plus large. Aussi longtemps, par exemple, que l'état de l'art photographique était tel que son image pouvait rarement être prise sans que l'on se soit consciemment "assis" dans ce but, le droit des contrats et de la confiance pouvait offrir à l'homme prudent des garanties suffisantes contre la circulation impropre de son portrait ; mais dès lors que les avancées les plus récentes dans l'art de la photographie ont rendu possible la prise de photographies à l'insu de la personne photographiée, les doctrines du contrat et de la confiance sont devenues inadéquates comme support à la protection requise et la responsabilité civile doit entrer en jeu » (op. cit., § 22).

109 Thomas Cooley, Cooley on Torts, 2nd ed., 1888, p. 29 : 3d ed., by John Lewis, 1st Vol., 1906, p. 33.

110 Union Pacific Ry. C. v. Botsford, 141 U.S. 250, 251 (1891) : victime d'un accident de chemin de fer, une femme avait refusé de déférer à la demande d'examen médical auquel prétendait la soumettre la compagnie de transport contre laquelle elle avait agi en responsabilité civile. Devant la Cour Suprême, le rejet de la demande d'expertise était confirmé aux motifs suivants : « Aucun droit n'est plus sacré, ni plus soigneusement protégé par le common law, que le droit de tout individu à la possession et au contrôle de sa propre personne, libre de tout contrainte ou de toute immixtion d'autrui, sauf en vertu de l'autorité claire et indiscutable de la loi. Comme l'a bien dit le juge Cooley : "le droit d'une personne sur elle-même peut être tenu pour un droit d'absolue immunité ; le droit d'être laissé seul" ».

111 Sur le fonctionnement du common law, v., dans cet ouvrage, F. Viangalli.

112 Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902).

qu'aucun précédent n'offrait une action dans l'espèce qui leur était soumise, ils s'en remettaient donc au législateur : « Le corps législatif pourrait très bien intervenir et disposer librement que nul ne devrait être autorisé, pour servir ses propres intérêts égoïstes, à utiliser l'image ou le nom d'autrui à des fins publicitaires, sans le consentement inconditionnel de la personne concernée. En cette hypothèse, le système juridique ne connaîtrait aucun embarras, puisque la loi serait applicable aux seules espèces visées expressément par le texte de loi »[113]. En 1903, le législateur de l'État de New York répondit à l'invitation lancée par les juges dans l'affaire *Roberson* et vint consacrer une *privacy tort action* par le *New York Civil Rights Act*, toujours en vigueur[114]. En 1905, enfin, la Géorgie devint le premier État à consacrer une action en responsabilité civile pour atteinte à la vie privée fondée sur le *common law*[115].

14. Soixante-dix années après la publication de l'article de Warren and Brandeis, William Prosser devait proposer, dans un article au moins aussi célèbre[116], la synthèse de près de trois cents affaires de responsabilité mettant en jeu la vie privée. Identifiant, à l'intérieur du *right to privacy*, quatre sortes d'atteintes distinctes portées à quatre intérêts différents, n'ayant en commun que de représenter une interférence avec le droit du plaintif d'« être laissé tranquille » (« *the right to be let alone* »)[117], il proposait la consécration de quatre *torts*. Lorsque le premier *Restatement of Tort* fut adopté en 1960, l'*American Law Institute* n'en consacra qu'un seul. Mais ces travaux exercèrent par la suite une telle influence que, en 1976, sa classification quadripartite se trouva finalement retenue dans le *Restatement (Second) of Torts*. Selon la disposition générale du paragraphe 652A(1), quiconque s'ingère dans la vie privée d'autrui est responsable du préjudice qu'il a causé à l'intérêt d'autrui. Le texte reconnaît ensuite (§652A(2)) quatre formes d'ingérences, qui correspondent donc aux quatre *torts* identifiés par Prosser[118] :

---

113 À la suite de cette décision, une note anonyme parue dans les colonnes de la Columbia Law Review critiqua vivement la prudence excessive des juges, observant qu'elle revenait à permettre à la presse de fouiller dans les faits les plus privés d'une personne et de les exposer grossièrement au public (« An Actionable Right to Privacy ? », 12 Yale L.J. 34 (1902)). L'un des juges de la majorité défendit son jugement dans le Yale Law Journal : D. O'Brien, « The Right to Privacy », 2 Colum. L. Rev. 486 (1902).

114 N.Y. Civ. Rights Act, art. 5, § 51, Action for Injunction and for Damages.

115 Pavesich v. New England Life Insurance Co., 50 S.E. 68 (Ga. 1905).

116 W.L. Prosser, « Privacy », 48 Cal. L. Rev. 383 (1960).- En réalité, Prosser avait partiellement dégagé cette typologie dans des écrits antérieurs, en particulier dans son traité de responsabilité civile : W.L. Prosser, Handbook of the Law of Torts, 1st ed., West Publishing Co., St. Paul, 1941 ; Handbook of the Law of Torts, 2nd ed., 1955 ; après le Restatement : v. W.L. Prosser, Handbook of the Law of Torts, 4th ed., West Publishing Co., St. Paul, 1971 ; cf. N.M. Richards, D.J. Solove, « Prosser's Privacy Law : A Mixed Legacy », 98 Cal. L. Rev. 1887 (2010), spéc. p. 1898-1900.

117 Dans le texte de 1960, il s'agissait des catégories suivantes : 1° Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs ; 2° Public disclosure of embarrassing private facts about the plaintiff ; 3° Publicity which places the plaintiff in a false light in the public eye ; 4° Appropriation, for the defendant's advantage, of the plaintiff's name or likeness (v. la traduction infra).

118 La traduction qui suit est due à É. Zoller, « Le droit au respect de la vie privée aux États-Unis », in F. Sudre, Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme, Bruylant, Bruxelles, 2005, p. 35-67, spéc. p. 40.

1. L'intrusion, matérielle ou non (*physically or otherwise*), dans l'intimité ou la solitude de l'individu à condition qu'elle soit manifestement offensante pour toute personne raisonnable[119] ;

2. L'appropriation de l'image d'une personne ou de sa ressemblance avec autrui[120] ;

3. La révélation au public de faits qui relèvent manifestement de la vie privée d'autrui à condition que ces faits soient de nature à choquer toute personne raisonnable et qu'ils ne présentent pas d'éléments de nature à éveiller un intérêt légitime dans le public[121] ;

4. La publication d'informations fausses et inexactes faisant apparaître l'individu sous un jour défavorable (*false light tort*)[122] .

La plupart des États fédérés reconnaissent ces cas de responsabilité, en tout ou partie[123]. S'ils ont constitué un très net progrès dans la protection de la vie privée aux États-Unis, ils restent, pour des raisons diverses, souvent insuffisants et font l'objet de critiques sévères[124] auxquelles n'échappe pas le troisième *tort*, le seul qui sera étudié dans le cadre de cette étude sur le droit à l'oubli[125].

15. Le droit des *torts* offre encore quelques ressources au-delà des *privacy torts*. Il faut mentionner les délits de diffamation et de calomnie (*torts of libel and slander*), institutions très anciennes qui permettent de retenir la responsabilité de celui qui, par la suite d'une fausse déclaration à propos d'une personne, a porté une atteinte à sa réputation[126] ; ou bien encore le *tort*

---

119 Restatement (Second) of Torts § 652(D) (1977).

120 Restatement (Second) of Torts § 652B (1977).

121 Restatement (Second) of Torts § 652E (1977).

122 Restatement (Second) of Torts § 652C (1977).

123 Même les États qui n'ont pas reconnu ces torts par la voie légale ont souvent fini par bénéficier d'une reconnaissance par la voie du common law. V., en particulier, pour le Minnesota : Lake v. Wal-Mart Stores, Inc. 582 N.W.2d 231 (Minn. 1998) : « Aujourd'hui, une très large majorité d'États reconnaissent une forme de droit à la vie privée. Seuls le Minnesota, le Dakota du Nord et le Wyoming n'ont reconnu aucun des quatre cas de responsabilité civile pour atteinte à la vie privée <four privacy torts>. Bien que les cours des États de New York et du Nebraska aient refusé de reconnaître au droit à la vie privée un fondement tiré du common law et aient préféré une protection législative, nous rejetons la proposition selon laquelle seul le législateur serait à même de créer de nouvelles actions <causes of action>. Le droit à la vie privée est inhérent à la protection que le droit anglais accorde à la propriété individuelle et aux droits de nature contractuelle, et le "droit d'être laissé seul" <right to be let alone> est reconnu comme partie intégrante du common law à travers le pays. Aussi est-il de la compétence du pouvoir judiciaire d'établir des cas de responsabilité pour atteinte à la vie privée dans cette juridiction ».

124 V. le colloque organisé, en 2010, par la California Law Review et qui s'est tenu à la Berkeley Law School à l'occasion du cinquantième anniversaire de la publication du célèbre article de Prosser (v. supra, note (115)). Cf., en particulier, L.J. Strahilevitz, « Reunifying Privacy Law », 98 Cal. L. Rev. 2007 (2010) ; N.M. Richards, D.J. Solove, « Prosser's Privacy Law : A Mixed Legacy », 98 Cal. L. Rev. 1887 (2010). Favorables à la classification de Prosser : P.M. Schwartz, L.-N. Peifer, « Prosser's Privacy and the German Right of Personality : Are Four Privacy Torts Better than One Unitary Concept ? », 98 Cal. L. Rev. 1925 (2010) ; v. aussi V. Mayer-Schönberger, « Beyond Privacy, Beyong Rights - Toward a "Systems" Theory of Information Governance », 98 Cal. L. Rev. 1853 (2010).

125 V. infra, n° 32 et s.

126 D. Solove, P. Schwartz, Information Privacy Law, op. cit., p. 32.

pour *infliction of emotional distress* qui reconnaît une action lorsqu'une personne, « par une conduite extrême ou scandaleuse a, sciemment ou par imprudence, causé une grave détresse émotionnelle à autrui »[127]. Si le texte peut parfois s'appliquer à des atteintes portées à la vie privée, son utilité est considérablement limitée par l'étroitesse de ses conditions d'application. La responsabilité peut encore découler de dispositions contractuelles spécifiques empêchant la collecte, l'usage ou la diffusion d'informations personnelles. En certaines hypothèses, les juridictions ont reconnu des actions pour violation de contrats implicites (« *actions for breach of implied contract* »)[128] ou des actions en responsabilité (*tort actions*) fondées sur des devoirs implicites (« *implicit duties* »), une fois du moins que certaines relations de confiance (« *fiduciary relationships* »), comme entre médecin et patient, ont pu être établies[129]. Des règles de confidentialité ainsi que des contrats de service contenant des dispositions relatives à la vie privée ont du reste parfois été analysées, par la doctrine, comme étant des contrats[130].

16. Il faut terminer en évoquant les diverses dispositions législatives adoptées à compter de la fin des années 1960. La période est marquée par de nombreux débats provoqués par l'apparition et le déploiement de nouvelles techniques, comme les écoutes téléphoniques[131] ou bien encore l'informatique[132], à l'origine de réactions inquiètes dans l'opinion publique. En 1973, un rapport très influent est rendu par le *United States Department of Health, Education, and Welfare* (HEW) à la suite d'un vaste audit des systèmes de traitement de données aux États-Unis[133]. Constatant des défaillances, le Département recommanda, notamment, l'édiction d'un *Code of Fair Information Practices*. Ces *Fair Informations Pratices*, qui ont « joué un rôle significatif dans la formation des lois relatives la vie privée aux États-Unis »[134], consistent dans un certain nombre de principes élémentaires relatifs à la vie privée informationnelle qui déterminent les droits et responsabilités dans la collecte et l'utilisation des données personnelles. En particulier, aucun système de conservation de données personnelles (« *personal-data record-keeping* ») ne devrait être tenu secret ; chacun doit disposer des moyens de connaître quelle information sur lui-même est

---

127 Restatement (Second) of Torts § 46 (1977).

128 V. aussi infra, n° 48.

129 Le tort of breach of confidence permet d'agir en responsabilité lorsqu'un professionnel, soumis à une obligation de confidentialité, tel un médecin, un juriste ou un banquier, divulgue une information confidentielle de son patient ou client (D. Solove, P. Schwartz, op. cit., p. 32 et p. 144). Cette action est à rapprocher du tort of breach of confidentiality du droit anglais, tel que dégagé, par exemple, dans les affaires Prince Albert v. Strange (1849) 1 Mac. & G. 25 et Pollard v. Photographic Company, 1888 Ch. 345. Dans ces deux affaires, l'obligation était de nature contractuelle, mais les juges anglais ont déjà admis l'existence d'obligations délictuelles de confidentialité : Duchess of Argyll v. Duke of Argyll [1967] 1 Ch. 303.- V. aussi, dans cet ouvrage, F. Viangalli, p. 134.

130 Sur tous ces points, D. Solove, P. Schwartz, op. cit., p. 33-34 ; et infra, n° 53 pour la position de la jurisprudence.

131 V. not. Katz v. United States, 389 U.S. 347 (1967).- Et infra, n° 19.

132 V., en particulier, les réactions violentes provoquées par le projet, présenté en 1965, de créer un National Data Center chargé de regrouper, à des fins de recherche, les données collectées par différentes agences chargées des statistiques : cf. E.S. Dunn, Jr, « The Idea of a National Data Center and the Issue of Personal Privacy », The American Statistician, Vol. 21, No. 1, Feb., 1967 ; K. Rebecca, « Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants », Journal of Privacy and Confidentiality : Vol. 5: Iss. 1, Article 1 (2013).

133 Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens, July, 1973.

134 M. Rotenberg, « Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get) », Stan. Tech. L. Rev. 1, 44 (2001).

conservée et comment elle est utilisée ; chacun doit être mis en mesure d'empêcher qu'une information sur lui-même obtenue pour une finalité (« *purpose* ») soit utilisée ou rendue disponible pour d'autres finalités sans son consentement ; chacun doit disposer du moyen de corriger ou d'amender l'enregistrement d'une donnée nominative (« *identifiable information about him* ») ; enfin, toute organisation créant, maintenant, utilisant ou disséminant des enregistrements de données personnelles (« *dissiminating records of identifiable personal data* ») doit s'assurer de la fiabilité des données au regard de l'usage prévu et doit prendre toutes les précautions raisonnables pour éviter un usage indu/abusif (« *misuse* ») des données[135]. Ces principes ont souvent été repris dans les très nombreux textes adoptés par le Congrès à partir des années 1970, en particulier le *Privacy Act* de 1974[136], puis le *Cable Communications Policy Act* de 1984[137], le *Electronic Communications Privacy Act* de 1986[138], le *Health Insurance Portability and Accountability Act* de 1996[139], le *Children's Online Privacy Protection Act* de 1998[140], le *Gramm-Leach-Bliley Act* de 1999[141] ou bien encore le *CAN-SPAM act* de 2003[142]. Certains de ces textes seront présentés lors de l'étude de la vie privée informationnelle[143]. Leur abondance et leur spécialité montrent, en tout cas, en plus des dispositions déjà évoquées, la remarquable complexité et fragmentation du corpus américain de protection de la vie privée que la jurisprudence constitutionnelle n'a jamais réussi à unifier.

B- Une absence d'unification constitutionnelle

17. On cherchera déjà en vain une référence explicite à la *pricacy* au sein de la Constitution américaine[144]. La vie privée y est apparemment absente, ce qui peut surprendre dans la mesure où l'histoire du Nouveau Continent, des Pères Pélerins (*Pilgrims*), est celle de la conquête de la liberté

---

135 V. aussi, D. Solove, P. Schwartz, op. cit., p. 37.

136 Pub. L. No. 93-579, 5 U.S.C. § 552 a.- Ce texte fait également suite au scandale du Watergate : cf. L.J. Strahilevitz, « Reunifying Privacy Law », art. préc., p. 2024.

137 Pub. L. No. 98-549, 47 U.S.C. § 551.

138 Pub. L. No. 99-508 et Pub. L. No. 103-414, 18 U.S.C. § 2510-2522, 2701-2709.

139 Pub. L. No. 104-191.

140 Pub. L. No. 106-170, 15 U.S.C. § 6501-6506.

141 Pub. L. No. 106-102, 15 U.S.C. § 6801-6809.

142 Pub. L. No. 108-187.- Toutes les références proviennent de D. Solove, P. Schwartz, op. cit., p. 37-39 qui fournissent une liste beaucoup plus complète.

143 V. infra, n° 54 et s.

144 En revanche, certaines Constitutions étatiques protègent directement la vie privée : Constitution de la Californie (Cal. Const. art. I, § 1) : « Tous les hommes sont libres et indépendants par nature et ont des droits inaliénables. Parmi ceux-ci figurent la jouissance et la défense de la vie et de la liberté <liberty>, l'acquisition, la possession et la protection de la propriété, ainsi que la poursuite et la satisfaction de la sûreté, du bonheur et de la vie privée » (à la différence de la plupart des dispositions constitutionnelles étatiques, le droit à la vie privée garanti par la Constitution de l'État de Californie s'applique non seulement aux acteurs publics, mais également aux personnes privées (Hill v. NCAA, 865 P.2d 638 (Cal. 1994)) ; Constitution de l'Alaska (Alaska Const., art. I, § 22 Right of Privacy) : « Le droit des personnes à la vie privée est reconnu et ne peut être violé. Le législateur doit donner exécution à la présente section ». La Constitution de la Floride (Fla. Const. art. I, § 23) : « Toute personne physique a le droit d'être seul et libre de toute ingérence de l'État dans la vie privée des personnes, à moins qu'il en soit disposé autrement ailleurs ». V. aussi : Ariz. Const. art. II, § 8 ; Mont. Const. art. II, § 10 ; Haw. Const. art. I, § 6 ; Ill. Const. art. I, § 6, 12 ; La. Const. art. I, § 5 ; S.C. Const. art. I, § 10 ; Wash. Const. art. I, § 7 (exemples tirés de D. Solove, P. Schwartz, op. cit., p. 35-36).

sur l'oppression du monarque, le secret sur l'examen constant[145]. En prenant pour prisme ce rapport complexe à la Couronne anglaise, on perçoit toutefois à maints endroits la marque de la vie privée, que ce soit dans la Déclaration d'Indépendance, dans la Constitution, dans le *Bill of Rights* ou dans les 17 amendements adoptés par la suite. Mais il faut au préalable remonter le fil du temps, jusqu'à gagner la période qui précède l'Indépendance. La Guerre de sept ans, qui a opposé, entre 1756 et 1763, la Grande-Bretagne à une coalition formée de la France et d'Indiens d'Amérique pour le contrôle de l'Amérique du Nord, offre de remarquables perspectives[146]. Ne parvenant pas, par le système de taxes du *Sugar and Molasses Act* de 1733[147], à enrayer le commerce de la mélasse avec les îles contrôlées par les Français, les Allemands et les Espagnols, et a ainsi protéger son commerce, le Parlement britannique, qui ne pouvait se priver plus longtemps de cette importante source de revenus dans un contexte de guerre, devait prendre la décision radicale de recourir aux *writs of assistance*.

Adoptés un siècle plus tôt sous le règne de Charles II, les *writs of assistance* offraient aux percepteurs des impôts un outil d'une efficacité remarquable. Il autorisait des perquisitions générales, le titulaire du *writ* pouvant fouiller où bon lui semblait et qui bon lui semblait. Ils ne faisaient surtout l'objet d'aucun contrôle judiciaire. Bien qu'un tel *writ* fût délivré par un juge, le demandeur n'avait pas à remplir une déclaration sous serment (« *affidavit* ») précisant l'objet de la perquisition, ni même les raisons qui le conduisaient à requérir une telle mesure, pourtant si dangereuse pour les libertés individuelles. Tant que le *writ* produisait effet, il pouvait du reste être transféré d'un agent à un autre, sans autorisation judiciaire, et aucun contrôle *a posteriori* ne permettait d'apprécier la légalité des mesures entreprises[148]. En 1755, alors que s'intensifiaient les échanges entre belligérants, et que croissaient les besoins de revenues, les britanniques commencèrent à délivrer des *writs of assistance*, au Massachussetts, attribuant ainsi aux officiers locaux le pouvoir illimité de perquisitionner au hasard les bateaux, les entrepôts et même les domiciles privés. Ces pouvoirs furent utilisés sans ménagements ce qui, on l'admettra sans peine, suscita l'indignation des populations concernées – marins et marchands[149]. Le *writ* honni n'était

---

145 F.S. Lane, American Privacy : The 400-Year History of our Most Contested Right, Beacon Press, Boston, 2011, p. 1-2. À l'époque, le monarque anglais, Élisabeth 1er, était hostile à leurs croyances puritaines, et les Pères Pèlerins, qu'on appelait alors Séparatistes, furent contraints de se réunir en secret afin de se soustraire au regard fatal de la Couronne et de ses agents. En 1607, et pour échapper à cette contrainte, les Puritains émigrèrent en Hollande et, surtout, sur le Nouveau Continent. Si plusieurs facteurs ont pesé sur la décision des Pères Pèlerins de franchir l'Atlantique et de gagner le nouveau Continent, l'un d'eux a été déterminant et il forme la quintessence de la vie privée : la liberté de développer des idées libres et nouvelles dans tous les domaines de la vie humaine, y compris la religion, le mariage, la politique, l'emploi, l'éducation. Pour les pionniers, le Nouveau Continent offrait du reste de nouvelles opportunités d'isolement. Ainsi qu'on l'a dit, « la solitude était largement disponible en Amérique » et les perspectives d'expansion sans limites offraient de vastes espaces de vie privée que nul n'aurait pu trouver dans les cités et villes surpeuplées d'Europe (D. Flaherty, Privacy in Colonial New England, University Press of Virginia, Charlottesville, 1972, p. 1, 33).

146 F.S. Lane, op. cit., p. 9.

147 Cf. F.S. Lane, op. cit., p. 9.

148 T. Maclin, « When the Cure for the Fourth Amendment Is Worse Than the Disease », 68 S.Cal.L.Rev. 1 (1994), spéc. p. 8 ; S.J. Wasserstrom, L.M. Seidman, « The Fourth Amendment as Constitutional Theory », 77 Geo L.J. 19 (1998), spéc. p. 82.

149 Ces writs of assistance sont également célèbres pour le réquisitoire que leur a adressé James Otis, l'un des Pères fondateurs de la Constitution. Il faut rappeler que ces writs étaient soumis à une règle particulière : ils expiraient six

pas le seul brandon de discorde. Plusieurs actes furent ardemment dénoncés durant cette période, recevant même la sinistre appellation « *d'actes intolérables du Parlement* »[150].

18. Si la *privacy* a bien un sens, aux États-Unis, c'est avant tout la garantie de pouvoir jouir d'une sphère d'intimité hors de toute immixtion arbitraire (à la manière des « actes intolérables ») de l'État et de ses représentants[151]. Sous cette nouvelle lumière, la vie privée apparaît mieux dans le Troisième[152] et surtout le Quatrième amendement du *Bill of Rights* : « Le droit des citoyens d'être garantis dans leurs personnes, domiciles, papiers et effets, contre des perquisitions et saisies déraisonnables ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est pour un motif plausible, soutenu par serment ou déclaration solennelle, ni sans qu'y soit décrit avec précision le lieu à fouiller et les personnes ou choses à saisir ». Ce texte en particulier rappelle combien le droit à la vie privée s'est structuré, aux États-Unis, dans un rapport vertical (État-citoyens), bien plus que les rapports verticaux (particulier-particulier)[153], exprimant ce faisant une défiance naturelle vis-à-vis de l'État[154] qui doit s'autolimiter et ne pas intervenir dans les rapports privés[155]. Il souligne en même temps l'étroitesse des liens tissés entre *privacy* et intimité du *home* ou « chez soi ». Cette vision érémitique de la vie privée, presque propriétaire, a eu un impact fondamental sur la maturation du concept constitutionnel de vie privée, en particulier dans son premier domaine d'expression – la procédure pénale – et en inhibe toujours les évolutions.

C'est dans le cadre l'exécution de la loi pénale (« *law enforcement* ») que la *privacy* s'est vu d'abord reconnaître valeur constitutionnelle, ce qui n'a jamais fait le moindre doute dans la mesure où le

---

mois après le décès du monarque qui les avait autorisés. Le 25 octobre 1760, le roi George II décédait. Les writs arrivaient donc à échéance, et Charles Paxton, le superviseur en charge des perquisitions auprès du port de Boston, demanda à la Cour Supérieure du Massachussetts la délivrance de nouveaux writs sous l'autorité de George III, le nouveau roi. La demande de Paxton fit l'objet d'une vaste opposition formée par un groupe de marchands et l'affaire fut appelée à l'audience en février 1761. Cette audience est l'un des moments importants de l'histoire américaine. Au jour de l'introduction de la demande, Otis était encore avocat général près le gouverneur britannique de la colonie. Refusant, contre les intérêts du gouverneur, la délivrance du writ, il renonça à son office et accepta de défendre gracieusement la cause des marchands. À l'audience, Otis dénonça pendant cinq heures les writs of assistance comme étant « des instruments de servage, d'une part, et de vilénie de l'autre ».

150 On peut mentionner le Quartering Act de 1765.

151 V. déjà la Déclaration d'Indépendance (4 juillet 1776).

152 « Aucun soldat ne sera, en temps de paix, logé dans une maison sans le consentement du propriétaire, ni en temps de guerre, si ce n'est de la manière prescrite par la loi ».- Sauf indication contraire, toutes les traductions de la Constitution américaine sont tirées de É. Zoller, Les grands arrêts de la Cour suprême des États-Unis, 1re éd., Dalloz, Grands arrêts, Paris, 2010, p. 867.

153 V., en particulier, livrant une comparaison avec l'Europe, J.Q. Whitman, « The Two Western Cultures of Privacy : Dignity versus Liberty », 113 Yale L.J. 1151 (2004).

154 D. Solove, « Chapter 1.- A Brief History of Information Privacy Law », in J. M. Kristen (dir.), Proskauer on Privacy : A Guide to Privacy and Data Security Law in the Information Age, Practising Law Institute (PLI), New York, 2011, p. 1-5.

155 À peine d'être accusé de paternalisme ; v., en ce sens, à propos du Children's Online Privacy Protection Act (Pub. L. No. 106-170, U.S.C. § 6501-6506 ; v. infra, n° 61), Anita Allen (« Minor Distractions : Children, Privacy and E-Commerce », 38 Hous. L. Rev. 751 (2001), p. 775-776) qui a pu soutenir : « En interdisant la divulgation volontaire par des enfants qui n'ont pas obtenu le consentement de leurs parents, dans des hypothèses où parents comme enfants peuvent paraître insensibles aux atteintes à la vie privée et répugner à voir le gouvernement intervenir, le COPPA passe pour l'une des lois fédérales sur la vie privée les plus paternalistes et autoritaires qui soient ».

Quatrième amendement règlemente expressément les perquisitions et saisies, et par voie d'extensions prétoriennes, toute une série de techniques d'investigations des plus anciennes (écoutes téléphoniques) jusqu'aux plus récentes (dispositifs de géolocalisation). La matière, riche et complexe, ne saurait être détaillée dans le cadre de ces lignes, mais il importe d'insister sur la coloration domiciliaire dont la *privacy* a eu la plus grande peine à se défaire. Comme beaucoup d'autres droits, mais peut-être sans jamais atteindre à une telle intensité, le *common law* anglais s'est avant tout attaché à défendre le domicile contre toute intrusion non autorisée. Selon la formule célèbre qui apparaît en 1499[156], et qui sera reprise par le *Semayne's Case* de 1604, « *the man house is his own castle* »[157]. On est frappé par l'ambiguïté que conservent encore, presque trois cents ans plus tard, les premières affaires (et les suivantes)[158] mettant en jeu des atteintes à la vie privée. Dans un arrêt mis en évidence par le Professeur Rigaux, qui précède de dix ans l'article de Warren et Brandeis (qui ne le mentionnent pourtant pas), la Cour Suprême du Michigan condamnait à des dommages intérêts, sous la qualification de *trespass*, le médecin qui avait autorisé une personne à assister, à l'insu de la parturiente, à l'accouchement ayant eu lieu au domicile de celle-ci. Pour la juridiction, la « plaignante avait un droit protégé par la loi à l'intimité de son appartement en de telles circonstances < *plaintiff had a legal right to the privacy of her apartment at such a time*>, et le droit protège ce droit en requérant d'autrui qu'il le respecte et s'abstienne de toute violation ». Comme on le voit, le terme de *privacy* est profondément ambigu et ne mérite pas (encore) d'être rendu par vie privée. C'est *l'intimité* qui est ici visée et qui prend tout son sens accolé au substantif : « appartement »[159] – comme si était fondamentalement en jeu l'inviolabilité du domicile[160].

19. Les virtualités dangereuses de telles décisions[161] n'ont pas échappé aux observateurs les plus attentifs de la vie privée aux États-Unis, en tout premier lieu le juge Brandeis qui, dans une opinion dissidente sous l'arrêt *Olmstead*[162] de 1928, plaida pour un élargissement de la vie privée. En l'occurrence, la Cour Suprême avait refusé de soumettre les écoutes téléphoniques au régime du Quatrième amendement, au motif qu'il « n'y avait eu aucune entrée dans les maisons ou les bureaux des accusés » ; les juges s'étaient donc prononcés contre l'exclusion des preuves. Pour Brandeis, tout autre aurait dû être la solution, car « [Les Pères fondateurs] ont cherché à protéger les Américains dans leurs croyances, leurs pensées, leurs émotions et leurs sensibilités. Ils leur ont

---

156 « The Right To Privacy In Nineteenth Century America », 94 Harv. L. Rev. 1892 (1981), note (18), p. 1894.

157 Semayne's Case, 77 Eng. Rep. 194 (K.B. 1604) : « the house of every one is to him as his castle and fortress ».

158 V. infra, n° 165-166.

159 À rapprocher de l'expression : « the privacy of one's home » : l'intimité du chez soi (V° Privacy, in Harrap's Shorter – Dictionnaire, Londres, Paris, 1991).

160 F. Rigaux, « Première leçon.- La liberté de la vie privée : de l'éclosion à l'explosion », in F. Rigaux, La vie privée.- Une liberté parmi les autres ?, Larcier, Bruxelles, 1992, p. 1-20, spéc. p. 2.

161 V. aussi Boyd v. United States, 116 U.S. 616, 630 (1886), où la Cour déclare contraire à la Constitution une loi fédérale prétendant contraindre un contribuable à communiquer ses livres comptables. Les principes dégagés, dit la Cour, « s'appliquent à toute atteinte du gouvernement et de l'un de ses agents à l'inviolabilité du domicile et à l'intimité de la vie <the sanctity of a man's home and the privacies of life>. Ce n'est pas le fait de fracturer ses portes, de fouiller dans ses tiroirs qui constitue l'essence de l'atteinte, mais c'est l'atteinte à son droit indéfectible à la sécurité personnelle, à la liberté individuelle et à la propriété privée, alors que ce droit n'a jamais été perdu du fait de sa condamnation à une infraction – c'est l'atteinte à son droit sacré qui sous-tend et constitue l'essence du jugement de Lord Camden ».

162 Olmstead v. United States 277 US 438, 466 (1928).

donné contre le gouvernement le droit d'être laissé tranquille, droit qui subsume tous les autres et qui est le plus chéri parmi les hommes civilisés. Pour protéger ce droit, toute intrusion non justifiée du gouvernement dans la sphère privée de l'individu, quels que soient les moyens employés, doit être présumée constituer une violation du Quatrième amendement »[163]. Il faudra attendre près de quarante ans pour que la Cour Suprême se rallie à la thèse du juge Brandeis, à l'occasion de l'arrêt *Katz v. United States*, rendu en 1967[164], et grâce auquel « [l]e droit à la vie privée vole désormais de ses propres ailes »[165]. L'importance de cette décision se mesure également à l'aune des limitations réelles qu'elle comprend et des exceptions virtuelles qu'elle prépare. Les limitations réelles sont exposées par le juge Harlan, dans son opinion concordante. Même si la propriété, le domicile n'est plus visé, seulement l'homme, il *est nécessaire que l'homme soit « situé », qu'il y ait un espace auquel se référer*. Mais, plus encore – et c'est là que s'ébauchent les exceptions virtuelles –, cet espace doit être doublement « reconnu ». Comme l'énonçait le même juge, pour qu'on puisse parler « d'espace », il y a « une exigence bipartite : d'abord [il faut] que la personne ait exprimé une espérance réelle (subjective) d'intimité de la vie privée ; ensuite que cette espérance soit de celles que la société est prête à reconnaître comme étant raisonnables ». C'est dans cette décision que s'exprime, pour la première fois, la doctrine de « l'espérance raisonnable » ou « espérance légitime »[166].

20. Réalisant un contrôle *in concreto* et a *posteriori*[167], et en l'absence de toute disposition constitutionnelle générale garantissant la vie privée, tous ces précédents dégagés sur le fondement du Quatrième amendement n'ont aucune valeur au-delà des questions de procédure pénale. Le droit constitutionnel de la vie privée se construit à la manière d'un herbier dont chaque page enferme un nouveau taxon. Dans le domaine de la divulgation d'informations de nature privée – faits par ailleurs protégés par le *tort of public disclosure* ou par certains textes garantissant l'accès aux documents publics, comme le *Freedom of Information Act* (FOIA)[168] –, la jurisprudence de la Cour

---

163 Trad. É. Zoller, « Le droit au respect de la vie privée aux États-Unis », in F. Sudre, Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme, op. cit., spéc. p. 51

164 Katz v. United States, 389 U.S. 347 (1967) : « le Quatrième amendement protège les personnes, non les lieux. Ce qu'une personne expose en connaissance de cause au public, fût-ce dans sa propre maison ou dans son bureau, ne bénéficie pas de la protection du Quatrième amendement. Mais ce qu'il cherche à préserver pour son intimité, même dans un lieu normalement accessible au public, peut être constitutionnellement protégé ». En conséquence, ajoutait-elle, il est très « net que l'objectif de cet amendement ne peut être articulé autour de la présence ou de l'absence d'immixtion physique dans un lieu clos donné ».

165 É. Zoller, op. cit., p. 51.

166 Sur cette notion qu'il n'est pas possible de développer dans ces lignes, cf. O.S. Kerr, « Four Models of Fourth Amendment Protection », 60 Stan. L. Rev. 503 (2007) ; Lior Jacob Strahilevitz, « A Social Networks Theory of Privacy », 72 U. Chi. L. Rev. 919 (2005).

167 En ce sens que, exercé après entrée en vigueur de la loi, le contrôle porte sur un litige précis qui met en jeu des intérêts individuels bien définis. Il doit y avoir un « case » ou une « controversery » (Constitution E.U., art. III, sect. 2) pour que la Cour Suprême accepte d'examiner la conformité d'une loi à la Constitution. Le contrôle de constitutionnalité est diffus, en ce sens qu'il est concurremment exercé par toutes les juridictions, dont les juridictions étatiques, sous le contrôle de la Cour Suprême.- V. sur ces points, et en particulier sur le rôle de la Cour Suprême : F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, op. cit., spéc. n° 94-96.

168 Pub.L. 89–554, 80 Stat. 378. Ce texte relève de ce que la doctrine américaine appelle le « freedom of information law ». Chaque État dispose d'un texte équivalent qui réglemente l'accès aux documents détenus par les institutions publiques. La plupart de ces textes, souvent taillés sur le modèle du FOIA, intègrent des dispositions protectrices de

Suprême est composée de trois arrêts : les deux premiers ont été rendus la même année, en 1977, *Whalen v. Roe*[169] et *Nixon v. General Services Administrator*[170]. Le troisième en 2011 : *Nasa v. Nelson*[171]. Dans la première de ces affaires, un groupe de patients, agissant par voie d'injonction, contestait la constitutionnalité d'une loi new-yorkaise mettant en place un traitement de données personnelles pour la prescription de certains médicaments jugés dangereux. Les demandeurs se plaignaient du risque de divulgation d'informations personnelles et d'une atteinte possible à leur autonomie, certains patients pouvant refuser le traitement par crainte d'une mauvaise utilisation des données traitées et d'une stigmatisation en tant que dépendants aux médicaments. Quelques mois seulement après *Whalen*, la Cour Suprême devait se prononcer dans l'affaire *Nixon*. Après la démission de Nixon, le Président Ford ratifiait le *Presidential Recordings and Materials Act*[172], qui faisait obligation à l'Administration des services généraux (*General Services Administration ou GSA*) de placer sous séquestre des papiers et enregistrements du Président Nixon. En vertu de cet acte, le GSA devait traiter et trier le matériel et, avec l'approbation du Congrès, déterminer l'accès public à celui-ci. Comme le matériel privé de Nixon était mélangé avec des documents et pièces officiels, il était inévitable que des éléments privés soient portés à la connaissance de l'Administrateur et de l'équipe d'archivistes[173]. Entre autres choses, Nixon soutenait que cette loi violait son droit à la vie privée garanti par les Premiers, Quatrièmes et Cinquièmes amendements. Dans la récente affaire *Nasa v. Nelson*, enfin, était en jeu une procédure de contrôle d'antécédents établie à l'échelle fédérale que le Département du Commerce, conformément à une directive de George W. Bush, est venu étendre aux salariés des cocontractants privés de l'État fédéral ayant un accès prolongé aux installations fédérales. La procédure impliquait plusieurs formulaires. Dans le premier, des informations personnelles étaient recueillies auprès du salarié lui-même et ces formulaires étaient ensuite envoyés aux anciens employeurs et propriétaires, aux établissements scolaires fréquentés et aux références mentionnées. Le second devait être rempli par les anciens propriétaires et répondants auxquels étaient posées une série de questions portant sur l'intimité du salarié. Toutes ces informations étaient protégées par le *Privacy Act*, en vertu duquel le Gouvernement peut collecter des données qui sont « pertinentes et nécessaires » à la satisfaction d'une finalité « requise par la loi », mais qui n'autorise la divulgation des données personnelles sans le consentement du sujet que dans certains cas. Là encore, un groupe de salariés agissait par voie d'injonction, arguant que la loi, qui permettait la collecte et la divulgation d'informations personnelles, portait atteinte à leur vie privée.

21. Si dans les trois arrêts la Cour Suprême a décidé en faveur de l'État, le premier comporte des précisions importantes. Examinant, en particulier, le risque de divulgation que peut présenter l'accès à l'information par les employés du Département de la santé de l'État de New York, la Cour note que cet accès n'est pas très différent de celui qui était garanti sous le droit

---

la vie privée : v. D. Solove, P. Schwartz, Information Privacy Law, op. cit., p. 636-637 ; v. aussi : A.W. Branscomb, Who Owns Information? From Privacy to Public Access, Basic Books, New York, 1994, p. 8.

169 Whalen v. Roe, 429 U.S. 589 (1977).

170 Nixon v. General Services Administrator, 433 U.S. 425 (1977).

171 Nasa v. Nelson 131 S. Ct. 746 (2011).

172 Title I of Pub.L. 93-526, 88 Stat. 1695.

173 On trouvait, par exemple, des communications avec sa femme, avec un pasteur, son journal personnel sur une sorte de dictaphone et les fichiers personnels de la première Dame.

antérieur et, surtout, qu'il doit être mis en perspective avec les atteintes qui, pour être déplaisantes, n'en sont pas moins nécessaires dans le domaine de la santé publique. La révélation d'informations médicales privées à des médecins, des personnels d'hôpitaux, des compagnies d'assurance ou des agences spécialisées dans la santé publique forment souvent une partie essentielle des pratiques médicales modernes, même lorsque la révélation peut refléter défavorablement le caractère du patient. En conclusion, la Cour énonce : « Nous jugeons que ni l'incidence immédiate ni la menace que représentent les exigences d'identification du patient posées par la loi de l'État de New York sur les substances contrôlées de 1982, sur la réputation ou l'indépendance des patients auxquels les médicaments de l'Annexe II sont prescrits, n'est suffisante pour constituer une atteinte à l'un des droits ou libertés garantis par le quatorzième amendement ».

L'arrêt prend tout son sens à travers son riche *obiter dictum* (« *A final word about issues we have not to decided* »). Lucide, la Cour souligne qu'elle n'est pas ignorante de la menace que représente, pour la vie privée, la grande quantité d'informations personnelles qui sont numérisées dans des banques de données ou dans d'autres importants fichiers gouvernementaux. Un certain nombre de fonctions assurées par l'État (perception des impôts, distributions des droits sociaux, etc.) supposent la conservation ordonnée d'un grand nombre de données, la plupart d'entre elles étant personnelles dans leur caractère, et leur révélation potentiellement embarrassante ou préjudiciable. C'est du reste pour prévenir ces dangers, ajoute la Cour, que le droit de recueillir et d'utiliser de telles données à des fins publiques est typiquement accompagné de dispositions législatives ou réglementaires destinées à éviter des divulgations injustifiées ; et, conclut la Cour, « dans certaines circonstances, une telle obligation a sans doute sa source dans la Constitution ». En l'occurrence, toutefois, en ce qui concerne la loi de l'État de New York, il est suffisamment démontré qu'il y a eu une prise en compte appropriée des intérêts de l'individu dans sa vie privée. L'*obiter dictum* éclaire également le fondement possible de cette protection constitutionnelle et le régime qui lui est applicable. À un endroit dans l'arrêt, la Cour note que « [l]es affaires qui passent parfois pour avoir protégé la "vie privée" <*privacy*> ont en fait impliqué deux sortes d'intérêts. L'un est l'intérêt individuel à éviter la divulgation <*disclosure*> de questions d'ordre personnel, et l'autre est l'intérêt à demeurer indépendant en prenant certaines catégories de décisions importantes ». Dans un langage plus moderne, on dirait que la vie privée regroupe d'une part la vie privée personnelle ou informationnelle[174] et d'autre part la vie privée décisionnelle (vie privée-liberté), telle que dégagée par l'arrêt *Roe v. Wade*[175]. Or par cette référence à peine dissimulée à la

174 La doctrine américaine englobe souvent, sous le terme de « vie privée informationnelle » (« information privacy ») tout à la fois les questions de divulgation de faits intimes et le traitement des données personnelles (v., en ce sens l'ouvrage de D. Solove et P. Schwartz, Information Privacy Law). Par ailleurs, dans bien des cas, la notion d'« information personnelle » est prise dans son sens étroit, comme se référant à des données intimes, et non dans son sens large comme visant toutes les informations se rapportant à une personne physique identifiée ou pouvant être identifiée : sur la distinction, cf. C. de Terwangne, « Internet Privacy and the Right to Be Forgotten/Right to Oblivion », op. cit., spéc. p. 111.- Mais dans le sens retenu dans cet article, cf. A. Allen, « Constitutional law and privacy », in D. Patterson, A companion to philosophy of law and legal theory, Blackwell, Oxford, 1996, p. 139-155.

175 Roe v. Wade, 410 U.S. 113 (1973). Arrêt majeur et bien connu qui reconnaît à la femme enceinte, sous certaines conditions, le droit de mettre un terme à sa grossesse. À la différence de l'arrêt Griswold v. Connecticut (381 US 479 (1965)), portant sur la question voisine de la contraception, qui, pour des raisons politiques, fondait le droit à la vie privée sur la liberté qui s'évince des « clairs-obscurs » (« penumbras ») de la Constitution, à savoir la liberté que l'on

vie privée-liberté, ainsi que par la mention expresse de la *due process clause* du Quatorzième amendement, la Cour indique la nature du contrôle qu'elle entend exercer. Puisque, semble-t-il, un droit « fondamental » est en jeu, le contrôle pourrait être maximum (« *strict scrutiny* »)[176], et comme l'indique dans son opinion séparée le juge Brennan « [u]ne large dissémination de telles informations par des agents de l'État, impliquerait toutefois des droits à la vie privée constitutionnellement protégés, et ne serait probablement justifiée que par un intérêt impérieux de l'État <*compelling state interest*> » – la référence à *l'intérêt impérieux de l'État* renvoyant bien entendu au contrôle strict. L'arrêt *Nixon* a paru, à certains égards, confirmer la rigueur du contrôle[177]. Mettant en place un « *balancing test* » (mise en balance par opposition à un mode d'adjudication en « tout ou rien »[178]), la Cour relevait que la loi contestée était le moyen le plus restrictif pour sélectionner les documents d'intérêt public. Le contrôle de l'*ultima ratio* (the « *least restrictive means* » pour atteindre l'intérêt impérieux de l'État) est normalement le troisième critère du *strict scrutiny test* (« *the archival review procedure involved here is designed to serve important national interests . . . and the unavailability of less restrictive means necessarily follows from the commingling of the documents* »). Et pourtant, l'arrêt *Nelson* paraît en retrait. La Cour y énonce : « Nous supposons, sans décider, que la Constitution protège un droit à la vie privée du type évoqué dans *Whalen* et *Nixon*. Nous jugeons, cependant, que la partie contestée du contrôle des antécédents par le Gouvernement ne viole pas la Constitution en l'espèce ». Surtout, la Cour indique que, d'après l'arrêt *Whalen*, il n'est pas nécessaire que les mesures soient les moins restrictives pour atteindre l'intérêt poursuivi par le

---

trouve comprise dans les Premier, Troisième, Quatrième, Cinquième et Neuvième amendements, l'arrêt Roe v. Wade opte pour un fondement plus simple : « Ce droit à la vie privée, qu'on le trouve dans le concept de liberté personnelle du Quatorzième amendement et les limites aux pouvoirs des États qui en découlent, comme nous le pensons, ou, comme la cour de district l'a jugé, dans la réserve de droits que le Neuvième amendement promet au peuple, est de portée suffisamment vaste pour inclure la décision d'une femme de mettre ou non un terme à sa grossesse » (trad. É. Zoller, Les grands arrêts de la Cour Suprême des États-Unis, op. cit., § 29, n° 5, p. 431 ; v. aussi l'analyse, op. cit., n° 24 et s., p. 442 et s.). L'arrêt consacre ce qu'on appelle la vie privée décisionnelle ou vie privée-liberté. V. aussi F. Rigaux, La protection de la vie privée…, op. cit., p. 182-187.

176 Le contrôle strict est exercé lorsqu'une loi affecte des droits personnels tenus pour « fondamentaux », en particulier les droits protégés par le Quatorzième amendement qui forme la due process clause (sur celle-ci, cf. J.V. Orth, Due Process of Law.- A Brief History, University Press of Kansas, Lawrence, 2003). L'État ne peut alors les réglementer qu'en justifiant d'un intérêt impérieux de l'État (Kramer v. Union Free School District, 395 U.S., 621, 627 (1969) ; la règlementation doit être rédigée « de manière suffisamment étroite pour ne servir que les légitimes intérêts de l'État qui sont en cause » (Griswold v. Connecticut, 381 US., 485 ; trad. É. Zoller, op. cit., § 29, n° 7, p. 433) et doit constituer le moyen le moins restrictif pour servir ces intérêts.

177 V., toutefois, les réactions contrastées des juridictions inférieures, infra, n° 23.

178 Selon l'expression du juge Frankfurter, dans son opinion concordante sous Dennis v. United States, 341 U.S. 494, (1951), spéc. p. 524-525 (cité par S. Van Drooghenbroeck, La proportionnalité dans la convention européenne des droits de l'homme.- Prendre l'idée simple au sérieux, Bruylant, Publications des Facultés universitaires Saint-Louis, Bruxelles, 2001, n° 907, p. 645). C'est ce que les auteurs américains appellent parfois le categorical balancing, par opposition au ad hoc balancing : S.H. Nahmod, « Public Employee Speech, Categorial Balancing and § 1983 : A Critique of Garcetti v. Ceballos », 42 U. Rich. L. Rev. 561 (2008) ; S. Tsakyrakis, « Proportionality : an Assault on Human Rights ? », 7 Int'L. J. Const. L. 468 (2010). Le plus souvent, cependant, la doctrine américaine tend à considérer qu'il n'y a pas de mise en balance derrière la première méthode qui consiste, simplement, à élaborer des catégories d'objets protégés ou non protégés (telle catégorie de discours, par exemple, en matière de liberté d'expression) : T.A. Aleinikoff, « Constitutional Law in the Age of Balancing », 96 Yale L.J. 943 (1987). On parle donc de categorical approach. On oppose nettement alors « Categoricalism » et « Balancing » : J. Blocher, « Categoricalism and Balancing in First and Second Amendment Analysis », 84 N.Y.L.Rev. 375 (2009).

Gouvernement. Les mesures doivent être « raisonnables », l'essentiel du contrôle se concentrant ensuite autour d'une mise en balance des intérêts.

22. Qu'en penser ? Plutôt que de structurer les deux précédents – *Whalen* et *Nixon* – autour d'un *balancing test*, il semblerait que la Cour Suprême ait souhaité, par son arrêt Nelson, reprendre une partie des critères dégagés par *Whalen* de manière à couper le lien, tissé par *Nixon*, avec la jurisprudence du Quatrième amendement et la doctrine de *l'espérance raisonnable de vie privée*[179]. Quant à la nature du contrôle, il semble que doive être distinguée l'hypothèse où la loi contestée menace directement la vie privée dans sa dimension « décisionnelle », c'est-à-dire « l'intérêt à demeurer indépendant en prenant certaines catégories de décisions importantes », en raison d'un risque de larges divulgations d'informations personnelles, de celle où la loi met en jeu « l'intérêt individuel à éviter la révélation <*disclosure*> de questions d'ordre personnel » en raison de l'atteinte possible à la « réputation ». Le *strict scrunity test* s'appliquerait seulement dans le premier cas, en raison de la mise en cause d'une liberté protégée par la *due process clause* ; un contrôle plus léger serait exercé dans le second. Une telle distinction manque évidemment de pertinence dans la mesure où la seule prise en compte de la nature de l'information (informations intimes, données sensibles, etc.), ainsi que l'ampleur des divulgations possibles (nombre d'informations en jeu, nombre de personnes y ayant accès), conduit à passer à côté du véritable enjeu. En raison de la « nature recombinante de l'information, des données peuvent constamment être agrégés entre elles, de même qu'à d'autres informations dont dispose le Gouvernement, de manière à révéler de plus larges informations à propos de l'individu »[180]. En somme, et comme l'a rappelé Daniel Solove, des informations, même anodines du point de vue de l'intimité ou de la réputation d'un individu, peuvent conduire à dresser un portrait relativement détaillé de la personne (tempérament, comportement)[181]. À travers le seul prisme de la réputation ou bien encore de la sécurité, comme l'ont parfois admis certaines juridictions[182], le risque que ces informations font courir n'apparaît pas. Il suffit pourtant de songer à ce qu'elles représentent pour l'identité et l'autonomie individuelles pour que s'ouvre un abîme de dangers. Enfin, même en reconnaissant un droit constitutionnel à la vie privée fondé sur la réputation, la Cour Suprême ne donne pas à la notion un contenu suffisamment ferme[183] pour lui permettre de triompher face aux intérêts antagonistes de l'État.

23. Les contours de la protection constitutionnelle de la vie privée sont incertains. Sans doute parce que la Cour Suprême n'a jamais souhaité unifier sa doctrine en privilégiant un

---

179 V. supra, n° 19-20.

180 Ch.P. Moniodis, « Moving from Nixon to Nasa : Privacy's Second Strand – A right to Informational Privacy », 15 Yale J. L. & Tech. 139 (2013), p. 159-160.

181

182 V. ainsi, dans le domaine des lois assurant l'accès aux documents publics : Kallstrom v. City of Columbus [Kallstrom I], 136 F.3d 1055 (6th Cir. 1998) (atteinte à la vie privée en raison de la divulgation d'informations pouvant porter atteinte à la sécurité de policiers agissant sous couverture) ; Kallstrom v. City of Columbus [Kallstrom II], 165 F. Supp. 2d 686 (S.D Ohio 2001) ; Barber v. Overton, 496 F.3d 449 (6th Cir. 2007).

183 Cf. Ch P. Moniodis, art. préc., spéc. p. 160-161, qui remarque que l'intérêt du citoyen qui est pris en compte est très abstraitement défini. La Cour Suprême porte également l'intérêt de l'État à un trop haut degré de généralité. Ce qui apparaît à chaque fois c'est la « national security » ou la « war on drugs » qui est visé. D'ailleurs, comme le note l'auteur, la sécurité devient un enjeu tout à fait fondamental et absorbant dans un monde post-11 septembre.

fondement et une méthode de contrôle. Dans le cadre de la mise en œuvre de la loi pénale (« *enforcement* »), la vie privée prend appui sur le Quatrième amendement, et si elle a réussi à se détacher de sa conception domiciliaire originelle, son déploiement a été considérablement limité par la doctrine de l'*espérance raisonnable* qui en constitue en quelque sorte le fondement actuel et modulable. Dans le domaine des traitements de données mis en œuvre par le Gouvernement, le fondement de l'*espérance raisonnable* paraît avoir été écarté[184], et une distinction contestable permet à la Cour Suprême de faire varier son contrôle : lorsque les données sont intimes, sensibles, la vie privée peut, en quelque sorte, se placer sous l'ascendant de la vie privée « décisionnelle » et bénéficier du contrôle strict initié dans le domaine des droits fondamentaux. Il va sans dire que les juridictions inférieures ont eu le plus grand mal à s'orienter en l'absence de lignes directrices claires. Certaines juridictions ont admis l'existence d'un droit constitutionnel à la vie privée informationnelle[185]. D'autres, en revanche, ont limité la protection constitutionnelle aux seules informations particulièrement sensibles ou intimes[186]. La nature et le niveau de contrôler à exercer restent des questions débattues[187] et certaines juridictions n'ont pas hésité à initier des raisonnements particuliers[188]. Enfin, le désordre est si grand que certaines juridictions ont paru douter de l'existence d'un droit constitutionnel à la vie privée informationnelle[189]. On verra que, cette question est encore compliquée par la jurisprudence constitutionnelle protectrice développée dans le cadre du *Freedom of Information Act* (FOIA), texte séminal en matière d'accès aux documents publics dans le cadre duquel la Cour Suprême a accordé une grande protection à la vie privée[190]. Malheureusement, cette jurisprudence remarquable ne vaut que pour le FOIA et pour l'articulation subtile qu'il assure entre vie privée et transparence.

II- L'articulation de la notion

24. Droit ou liberté, la vie privée doit s'articuler avec un certain nombre d'intérêts concurrents, ce que rappelle du reste avec force le débat actuel sur le droit à l'oubli. L'article 17 de

---

184 Une cour s'est toutefois fondée sur l'espérance raisonnable de vie privée pour déterminer si une information méritait d'être protégée par un droit constitutionnel à la vie privée informationnelle : Fraternal Order of Police, Lodge No. 5 v. Philadelphia 812 F.2d 105, 112 (3d Cir. 1987).

185 In re Crawford, 194 F.3d 954, 958 (9th Cir. 1999) ; Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990) ; Borucki v. Ryan, 827 F.2d 836, 846 (1st Cir. 1987) ; Mangels v. Pena, 789 F.2d 836, 839 (10th Cir. 1986).

186 Sterling v. Borough of Minersville, 232 F.3d 190, 194 (3d Cir. 2000) ; Herring v. Keenan, 218 F.3d 1171, 1173 (10th Cir. 2000) – v. toutefois : Borucki v. Ryan, 827 F.2d 836, 841 (1st Cir. 1987) : « it is not clear from Whalen whether, to be constitutionally protected by a right of nondisclosure, personal information must concern an area of life itself protected by either the autonomy branch of the right of privacy or by other fundamental rights or whether, to the contrary, the right of confidentiality protects a broader array of information than that implicated by the autonomy branch of the right of privacy ».

187 Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983) ; Plante v. Gonzalez, 575 F.2d 1119, 1132-34 (5th Cir. 1978) ; In re Paternity of K.D., 929 N.E.2d 863, 869 (Ind. Ct. App. 2010).

188 Smith v. City of Artesia, 772 P.2d 373, 376 (N.M. App. 1989) : le droit à la vie privée informationnelle « ressemble beaucoup, et pourrait donc être identique à l'intérêt protégé par l'interdiction posée par le common law de donner une publicité déraisonnable à la vie privée d'autrui <one's private life> » ; V. aussi le test en 7 facteurs mis en place par le troisième circuit : United States v. Westinghouse Electric Corp., 638 F.2d 570, 578 (3d Cir. 1980).

189 Cf. not. J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981).

190 United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989). V. infra, n° 30.

la proposition de règlement 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[191] prévoit ainsi, au titre des exceptions à l'effacement des données : l'exercice du droit à la liberté d'expression[192], des motifs d'intérêt général dans le domaine de la santé publique[193] et des motifs liés à la recherche historique, statistique et scientifique[194]. Aux États-Unis, plusieurs séries d'intérêts viennent contrebalancer les dispositions en matière de vie privée et de protection des données et sont susceptibles de s'opposer à l'exercice d'un droit à l'oubli. Tel est le cas des intérêts économiques dont on verra qu'ils permettent parfois la divulgation d'informations au mépris de la vie privée[195] ,

---

191 COM/2012/011 final - 2012/0011 (COD) (v. supra, n° 6).

192 Art. 80.

193 Art. 81.

194 Art. 83.

195 V. infra, n° 69.- Les services fournis par les grandes entreprises de l'Internet sont financés par la vente de données personnelles et la publicité comportementale. La vie privée peut donc être tenue en échec par les exigences du modèle économique appliqué : J.P. Nehf, « Incomparability and the Passive Virtues of Ad Hoc Privacy Policy », 76 U. Colo. Rev. 1 (2005), p. 29-36, p. 42 (reproduit par extrait in D. Solove, P. Schwartz, Information Privacy Law, op. cit., p. 912-913).- Un rapport récemment réalisé par le European Centre for International Political Economy (ECIPE), pour le Chambre américaine du Commerce (ECIPE, The Economic Importance of Getting Data Protection Right : Protecting Privacy, Transmitting Data, Moving Commerce, ECIPE, Brussels, 2013), met en évidence la possible position américaine vis-à-vis de la proposition de règlement sur la protection des données (sur celle-ci, v. supra, n° 6) et explique sans doute mieux l'intense lobbying des entreprises américaines auprès des institutions de l'UE (cf. G. Pépin, « Vie privée : des amendements de lobbyistes américains dans le projet de loi européen », Le Monde 12.02.2013, & http://lobbyplag.eu/map ; les autorités américaines seraient également intervenues : A. Debet, « Programme Prism : les citoyens européens sur écoute », D. 2013, p. 1736). Dans ce document d'analyse économique, qui prend place, faut-il le rappeler, dans le contexte de négociation du « partenariat transatlantique de commerce et d'investissement » (le nouvel accord de « libre-échange » entre l'Union européenne et les États-Unis), les rapporteurs soulignent l'impact que pourrait avoir l'adoption de la proposition de règlement sur les Safe Harbor Principles (« principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée »), adoptés par le Département américain du Commerce le 19 avr. 1999. Ces principes, rappelons-le, permettent les flux transfrontières de données, de l'Union européenne vers les États-Unis (directive 95/46/CE, art. 25, § 1 et 6 – ce système est évoqué infra, n° 87). L'entrée en vigueur d'un nouveau texte pourrait contraindre les entreprises américaines à adopter de nouveaux standards ou remettre en cause purement et simplement les Safe Harbor Principles. Le rapport envisage ces deux hypothèses en termes économiques et évalue enfin les conséquences que pourrait également avoir l'adoption du « droit à l'oubli » tel que prévu dans la proposition. Le premier scénario se traduirait par l'édification de barrières non tarifaires au détriment des États-Unis. Les exportations de service diminueraient de 0.2 à 0.5% (chiffres auxquels il faut ajouter une perte de compétitivité). Le deuxième scénario aurait pour effet d'empêcher les flux de données en direction des États-Unis. Les entreprises américaines devraient donc opérer depuis l'Union européenne, d'où une augmentation du coût des services (la main-d'œuvre qualifiée étant plus chère de 30% au sein de l'UE qu'aux États-Unis) qui se répercuterait sur les prix pratiqués (augmentation attendue : de l'ordre de 4 à 13%). Le troisième et dernier scénario, celui aboutissant à la mise en œuvre du droit à l'oubli, quoique perçu comme hautement improbable, aurait les effets suivants : pour les entreprises, le respect de la mesure coûterait globalement à un responsable de traitement entre 9 et 41 milliards d'euros ; pour l'UE, une diminution du PIB de l'ordre de 1.5% à 3.9%. V. les chiffres beaucoup plus optimistes de la Commission : Commission Staff Working Paper, Impacct Assessment, SEC (2012) 72 final, Brussels, 25.1.2012.- Adde, UK Ministry of Justice, Impact Assessment on Proposal for EU Data Protection Regulation, 22.11.2012.

des enjeux de sécurité publique dont l'importance n'est plus à démontrer[196], et dans une bien moindre mesure, les « droits de l'Histoire »[197].

Ce sont les enjeux démocratiques qui recouvrent, cependant, les deux intérêts les plus importants. Par enjeux démocratiques, il faut entendre, au sens large, *toutes les garanties qui s'attachent au bon fonctionnement des institutions publiques et au maintien de l'État de droit*[198]. Ce qui doit conduire à s'interroger sur l'articulation de la vie privée (et du droit à l'oubli) avec la liberté d'expression (A) et la transparence (B).

A- La liberté d'expression

25. Liberté d'expression (« *free speech* ») et liberté de la presse occupent une place singulière aux États-Unis dont on ne peut mesurer la portée sans mettre en évidence leur soubassement. Les mots que leur consacre le Premier amendement sont courts : « Le Congrès ne fera aucune loi [...] qui restreindrait la liberté de parole ou de presse [...] » ; mais ils expriment plusieurs idées d'une portée politique considérable. La première, que l'on trouve déjà chez Milton[199] et Stuart Mill[200], se trouve exprimée par le juge Holmes dans une célèbre opinion dissidente sous *Abrams v.*

---

196 La tension a toujours été grande, aux États-Unis, entre la vie privée et la sécurité. Mais le phénomène s'est amplifié à la suite des attentats du 11 septembre 2001. Pour un positionnement du problème, cf. D.J. Solove, Nothing to Hide.- The False Tradeoff between Privacy and Security, Yale University Press, New Haven, London, 2011.- V. aussi, supra, n° 21, les remarques formulées à propos de l'arrêt Nixon v. General Services Administrator, 433 U.S. 425 (1977).- Le sujet est plus que jamais d'actualité : cf. J. Tate, C.D. Leonnig, « NSA broke privacy rules thousands of times per year, audit finds ; Agency also has overstepped legal authority since Congress gave it broad new power in 2008 », Washington Post.com, 21 août 2013.

197 En amont de l'affaire Nixon v. General Services Administrator, 433 U.S. 425 (1977), un accord dit « Nixon-Sampson » avait été passé entre Nixon et l'Administrateur des services généraux. Il donnait au président démissionnaire le pouvoir de détruire certains de ses papiers et documents. Ce n'était pourtant pas là la pratique des anciens présidents et le Congrès s'en émut. Il annula l'accord, soulignant son désir de sauvegarder « l'intérêt du public dans l'accès approprié aux matériaux de la présidence Nixon, qui sont d'une importance historique générale » (H.R.Rep. No. 93-1507, p. 2 (1974)). Dans son opinion concordante sous Nixon, le juge White tint pourtant à rappeler la faiblesse de l'intérêt avancé sur ce point par l'État. Le § 104(a)(7) du Presidential Recordings and Materials Preservation Act, voté par le Congrès et discuté par la Cour Suprême, prévoyait notamment que les matériaux privés seraient rendus au président, du moins ceux qui « ne sont pas par ailleurs d'une importance historique générale ». Pour White, « [...] la validité de la loi [the Act] serait douteuse si, pour conserver des lettres purement privées ou des journaux intimes, il suffisait simplement d'en avancer l'importance historique générale ».

198 Sur le lien entre rule of law et transparence : É. Zoller, « Le principe de transparence et les nouvelles technologies de l'information aux États-Unis », Conférence-débat du CDPC sur la transparence administrative et ses déclinaisons technologiques récentes, Cycle « Les valeurs du droit public », 15 avr. 2013 (accessible en ligne).

199 J. Milton, Pour la liberté de la presse sans autorisation ni censure : Areopagitica, éd. bilingue, (trad. O. Lutaud), Aubier-Flammarion, Paris, 1969.

200 J. Stuart Mill, De la liberté (trad. Dupont-White), Guillaumin et Cie, Libraires, Paris, 1860, p. 93-94 : « 1° Une opinion qu'on réduirait au silence peut très-bien être vraie : nier ceci, c'est affirmer notre propre infaillibilité ; 2° quand même l'opinion réduite au silence serait une erreur, elle peut contenir, ce qui arrive la plupart du temps, une portion de vérité ; et puisque l'opinion générale ou dominante sur quelque sujet que ce soit est rarement ou n'est jamais toute la vérité, on n'a de chance de la connaître en entier que par la collision des opinions adverses ; 3° même dans le cas où l'opinion reçue contiendrait la vérité et toute la vérité, on la professera comme une sorte de préjugé, sans comprendre ou sentir ses principes rationnels, si elle ne peut être discutée vigoureusement et loyalement ; 4° le sens de la doctrine elle-même sera en danger d'être perdu, ou affaibli, ou privé de son effet vital sur le caractère et la

United States[201] : « L'ultime bien commun désiré est mieux atteint par le libre commerce/échange des idées <*free marketplace of ideas*> [et] le meilleur test de vérité se trouve dans le pouvoir des idées à se faire accepter dans la compétence du marché »[202]. La deuxième est due à Brandeis, champion de la vie privée, mais qui a reconnu, à la fin de sa vie, toute l'importance de la liberté d'expression, aux fins de permettre, en particulier, le libre épanouissement individuel au sein de l'État : « Ceux qui ont gagné notre indépendance pensait que la fin ultime de l'État était de rendre les hommes libres de développer leurs facultés ; et que dans son gouvernement les forces délibératives devaient l'emporter sur les forces arbitraires. Ils ont défendu la liberté tout à la fois comme une fin et un moyen. Ils ont pensé que la liberté était le secret du bonheur et le courage le secret de la liberté »[203]. Enfin, des théories plus modernes soulignent l'importance du *libre discours* et de la liberté de la presse dans le contrôle de l'exercice du pouvoir par les agents de l'État[204]. Probablement aucun autre système constitutionnel n'a accordé autant de poids à cette liberté et n'a traité avec autant de rigueur toute entrave susceptible d'en compromettre l'existence ou limiter l'exercice, dont la vie privée et toute forme possible de droit à l'oubli[205]. Comme ces questions d'articulation entre liberté d'expression et vie privée (ou traitement des données personnelles) forment le cœur des prochains développements, nous pouvons les délaisser pour l'heure, en ayant toutefois précisé au préalable que vie privée et liberté d'expression ne s'opposent pas toujours, la seconde pouvant parfois venir protéger la première. C'est ainsi que, renforcée par la liberté d'expression, la vie privée assure le droit de parler de manière anonyme (*McIntyre v. Ohio Election Comm'n*, 514 U.S. 334 (1995)). Par ailleurs, la liberté d'association, garantie par le Premier amendement, met les individus à l'abri de toute demande visant à obtenir la révélation des groupes auxquels ils appartiennent ou contribuent. La Cour Suprême a aussi bien censuré une loi faisant obligation de dévoiler le nom et l'adresse des membres d'une organisation (*NAACP v. Alabama*, 358 U.S. 449 (1958)). Elle a réservé le même sort à une loi exigeant des enseignants publics de dresser une liste de toutes les organisations auxquelles ils appartiennent ou participent (*Shelton v. Tucker*, 364 U.S. 479 (1960)).

---

conduite ; car le dogme deviendra une simple formule, inefficace pour le bien mais encombrant le terrain et empêchant la naissance de toute conviction réelle fondée sur la raison ou sur l'expérience personnelle ».

201 Abrams v. United States, 250 U.S. 616, 630, 40 S.Ct. 17, 22, 63 L.Ed. 1173 (1919) (opinion dissidente).

202 Le terme de commerce doit être pris dans son sens, aujourd'hui vieilli, d'« échange » (cf. É. Littré, Dictionnaire de la langue française, Hachette, Paris, Londres, 1876-1878, V° Commerce ; et v. trad. alternative : É. Zoller, Les grands arrêts de la Cour Suprême des États-Unis, op. cit., p. 630) ; la coloration économique n'est pas absente, comme le suggère la seconde partie de la citation.

203 Brandeis, J., opinion concordante : Whitney v. California, 274 U.S. 357, 47 S.Ct. 641, 71 L.Ed. 1095 (1927).- À cette idée s'adjoint celle selon laquelle la santé d'une Nation souveraine est entretenue par les contributions de chacun des individus qui la composent : cf. L.C. Bollinger, « Free Speech and Intellectual Values », 92 Yale L.J. 438 (1983).

204 V. Blasi, « The Checking Value in First Amendment Theory », 1977 A.B. Foundation Res.J. 521.- V. aussi : R.D. Nowak, J.E. Rotunda, Treatise on constitutional law : substance and procedure, Thomson/West, éd. électr. Westlaw, 2013, § 20.6(f).- Et voir, sous l'angle du droit à l'oubli : R.G. Larson III, « Forgetting the First Amendment : How Obscurity-Based Privacy and a Right to be Forgotten are Incompatible with Free Speech », 18 Comm. L. & Pol'y 91 (2013), spéc. p. 108 et s.

205 Sur les réactions passionnées de la presse américaine à la proposition de règlement, v. P.A. Bernal, « A Right to Delete ? », European Journal of Law and Technology, vol. 2, No. 2 (2011), spéc. § 1.2.- Et v., plus largement, M.L. Ambrose, J. Ausloos, « The Right to Be Forgotten Across the Pond », Journal of Information Policy 3 (2013), 1-23, spéc. note (2).

B- La transparence

26. La transparence – l'accès aux documents publics – crée une autre tension avec la vie privée et un possible droit à l'oubli. La question est importante, car la réglementation de l'accès donné aux citoyens à un certain nombre d'informations contenues dans des fichiers de l'administration et les dossiers judiciaires forme le poste avancé du contrôle des données et permet au temps d'opérer ses vertus d'inhibition progressive[206]. Elle ne règle pourtant pas toutes les difficultés, la liberté de la presse venant parfois détruire, ainsi que nous le verrons[207], le subtil équilibre dégagé par le droit en matière d'accès – ce qui appelle de nouveaux arbitrages.

La problématique de la transparence se donne pleinement à voir à travers les questions d'accès aux dossiers judiciaires et aux fichiers publics. Selon une jurisprudence bien établie, la « transparence judiciaire » (« *judicial openness* ») comporte deux volets : le droit d'assister aux procès eux-mêmes et le droit d'accéder aux documents judiciaires pour examen et copie[208]. Le premier a valeur constitutionnelle en ce qu'il se trouve implicitement garanti par les Premier et Quatorzième amendements[209]. Quant au second, s'il est incontestablement reconnu par le *common law*[210], sa valeur constitutionnelle est discutée[211], ce qui laisse en particulier incertaines les limites portées à l'accès au dossier judiciaire et les restrictions qui pourraient accompagner le processus de numérisation des archives judiciaires. En tout état de cause, l'accès public au dossier judiciaire peut se réclamer d'exigences fondamentales : contrôle de l'activité des tribunaux, éducation des justiciables et maintien de la confiance du public dans le système judiciaire[212]. Ainsi s'explique la présomption favorable dont jouit l'accès public au dossier judiciaire[213]. Ce dossier judiciaire (« *court record* ») forme l'une des catégories de ce grand ensemble que constituent les documents publics ouverts au public[214]. À l'échelle fédérale, l'accès ne se fait pas sur le fondement du *FOIA* (examiné ci-après) – qui ne s'applique qu'aux dossiers constitués et traités par le pouvoir exécutif[215] –, mais d'un texte spécifique[216]. Sauf exceptions qu'il va falloir préciser, tout citoyen

---

206 V., en droit français : L. 29 juillet 1881 sur la liberté de la presse, § 5 Publications interdites, immunités de la défense. Cf. N. Mallet-Poujol, « Presse en ligne et droit à l'oubli numérique : nouvelles responsabilités », in É. Vergès (dir.), Droit, sciences et techniques : quelles responsabilités, op. cit., p. 283 et s.

207 V. infra, n° 42 et s.

208 Cf. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 580 (1980) ; United States v. Gotti, 322 F. Supp. 2d 230, 239 (E.D.N.Y. 2004).

209 Richmond Newspapers, Inv. v. Virginia, préc.

210 Nixon v. Warner Communications, Inc., 435 U.S. 589, 597 (1978).

211 Zenith Radio Corp. v. Matsushita Elec. Indus. Co., 529 F. Supp. 866, 897 (E.D. Pa. 1981) ; Brown & Williamson Tobacco Corp. v. FTC, 710 F.2d 1165, 1176-81 (6th Cir. 1983).- Contra : Republican Co. v. Appeals Court, 812 N.E.2d 887, 892 (Mass. 2004).- V. aussi, N. Gomez-Velez, « Internet Access to Court Records – Balancing Public Access and Privacy », 51 Loy.L.Rev. 365 (2005), spéc. p. 403 et s.

212 N. Gomez-Velez, op. cit., p. 369.

213 Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978).

214 A. Conley et alii, « Sustaining Privacy and Open Justice in the Transition to Online Court Records : A Multidisciplinary Inquiry », 71 Md. L. Rev. 772 (2012), spéc. p. 784-785.

215 V. désormais le E-Government Act de 2002, qui s'applique aux trois branches de Gouvernement, et donc aux juridictions fédérales : E-Government Act of 2002, Pub. L. No. 107-347, § 205(a)-(b), 116 Stat. 2910, 2913-14 (codifié : 44 U.S.C. §3501 (2006)).

peut accéder à un nombre considérable de pièces, dont l'acte introductif d'instance, les conclusions en réponse (et demandes reconventionnelles), les pièces, documents et objets présentés devant la juridiction pour examen, ainsi que la transcription des débats et l'opinion de la juridiction. Ce nombre peut encore augmenter en fonction des demandes (« *motions* ») introduites[217] au cours de la procédure. Des informations telles que le numéro de sécurité sociale (« *social security number* » – *SSN*), l'adresse du domicile, le nom des enfants mineurs, les numéros de comptes bancaires ou bien encore des informations médicales particulièrement sensibles peuvent se trouver divulguées par ce biais.

27. Un moyen d'éviter la dissémination d'informations intimes ou de données personnelles est de recourir à l'anonymat ou au pseudonymat. La question s'est posée à plusieurs reprises pour des victimes d'agressions sexuelles qui, dans le cadre d'actions en responsabilité civile[218], entendaient conserver leur anonymat. D'après la règle 10(a) des *Federal Rules of Civil Procedure*, l'acte introductif d'instance (« *complaint* ») doit contenir le nom de toutes les parties. L'intention du texte est de permettre aux parties de connaître leurs adversaires, mais aussi de protéger « l'intérêt public légitime dans la connaissance des faits compris dans le débat »[219]. Les juridictions conservent, néanmoins un pouvoir étendu (qualifié de « discrétionnaire ») qui leur permet d'accorder à un litigant le droit d'agir ou de défendre anonymement[220]. Dans l'affaire *Doe v. Sakur*[221], la Cour a précisé que, dans la mise en balance de l'intérêt attaché à l'accès et celui attaché à la vie privée, il convenait de tenir compte des facteurs suivants : *(1) le plaignant entend-il contester une activité gouvernementale ; (2) le plaignant doit-il divulguer des informations très intimes ; (3) le plaignant serait-il contraint de faire aveu de son intention de prendre part à une activité illégale, risquant par cela des poursuites criminelles ; (4) le plaignant risque-t-il un dommage s'il est identifié ; (5) la partie devant se défendre contre une action introduite sous pseudonyme risque-t-elle d'en être affectée négativement ?*

Les juridictions ne sont pas toujours sensibles à l'intégralité de ces facteurs, mais toutes tiennent évidemment compte du risque que l'anonymat du demandeur (ou du défendeur) fait peser sur l'équité de la procédure[222], de l'intérêt public dont peut se réclamer éventuellement le plaideur qui

---

216 Dans certains cas, l'accès se fait simplement sur le fondement du common law : N. Gomez-Velez, art. préc., spéc. p. 407.

217 Pour une analyse détaillée, cf. A. Conley et alii, op. cit., loc. cit., p. 778-779.

218 En matière pénale, les règles sont différentes, car les textes pertinents ferment souvent l'accès au dossier. Par ex., en vertu de l'article 160 de la New York Criminal Procedure Law, le dossier d'une affaire criminelle est rendu confidentiel lorsque la procédure aboutit à la relaxe ou l'acquittement complet de la personne poursuivie ou lorsque l'affaire fait l'objet d'un rejet (« dissimal ») pour des motifs constitutionnels (violation du droit d'être jugé dans un délai raisonnable) ou pour insuffisance des preuves. L'article 720.35(2) prévoit également la confidentialité du dossier en matière de poursuites pénales contre un mineur.

219 Doe v. Shakur, 164 F.R.D. 359 (S.D.N.Y 1996).

220 Doe v. Bell Atlantic Business Sys. Servs., Inc., 162 F.R.D. 418, 420 (D. Mass. 1995) ; United States v. Microsoft Corp., 56 F.3d 1448n 1463-1464 (D.C. Cir. 1995) (per curiam).

221 Précitée.

222 Doe v. Shakur, 164 F.R.D. 359 (S.D.N.Y 1996) : où la Cour note que la demanderesse a choisi d'introduire une action en responsabilité civile. Les charges sont graves et elle a mis sa crédibilité en jeu. L'équité (« fairness ») commande qu'elle soutienne ses charges publiquement. Plus loin, elle observe que le défendeur a été publiquement accusé. Si la demanderesse était autorisée à mener son action de manière anonyme, le défendeur se trouverait dans une position de très net désavantage, puisqu'il lui faudrait se défendre publiquement, tandis que la demanderesse

demande l'anonymat[223], de l'importance que représente, enfin, pour le public, l'accès à la justice, car « les actions en justice sont des événements publics et le public a un intérêt légitime à connaître les faits qui s'y jouent. Parmi ces faits figure l'identité des parties »[224]. Dans une affaire mettant en jeu la divulgation possible du dossier psychiatrique d'un plaideur atteint de troubles obsessionnels compulsifs, la juridiction, rejetant en l'occurrence la demande d'anonymat[225], a du reste laissé entendre que le demandeur à la mesure devait se prévaloir de faits de nature à marquer la personne du sceau de l'infamie ou de l'humiliation ou, pour le moins, d'une pathologie dont la divulgation pourrait être « hautement embarrassante » pour une personne moyenne[226]. D'autres moyens existent encore, comme les « *protective orders* »[227] ou « *sealing orders* »[228] qui permettent d'obtenir du juge la confidentialité[229] de certaines informations, les *sealing agreements* qui, négociés par les avocats des parties et homologués par le juge, permettent de retirer du dossier certaines informations[230] ou bien encore certaines dispositions qui empêchent l'accès au dossier de certaines procédures[231].

---

pourrait se dissimuler derrière le « voile de l'anonymat » ; Doe No. 2 v. Kolko, 242 F.R.D. 193 (2006) : il n'est pas démontré, note la Cour, que le défendeur ne serait pas en mesure de mener correctement la procédure de discovery ou de mettre en cause, le cas échéant, la crédibilité du demandeur.

223 Il peut s'agir du besoin de prévenir des représailles ou de l'intérêt public dans la protection des victimes d'abus sexuels (Doe No. 2 v. Kolko, préc). Dans l'affaire Doe v. Shakur, la Cour notait, au contraire, que l'intérêt poursuivi par l'action en responsabilité civile étant un intérêt personnel, on ne pouvait appliquer par analogie les lois (« rape shield laws ») qui, en matière pénale, assurent l'anonymat des victimes afin de les inciter à témoigner.

224 Doe v. Shakur, préc.

225 Doe v. Blue Cross & Blue Shield United of Wisconsin, 112 F.3d 869 (7th Cir. 1997) : la cour note plaisamment qu'il s'agit d'un trouble courant, dont souffrent d'ailleurs, jusqu'à un certain point, beaucoup de juges et de juristes !

226 Ibid.

227 Les « protective orders », qui sont des ordres de non-production délivrés par la juridiction, peuvent être obtenus durant la phase de discovery, de manière à éviter la divulgation de certaines informations. À l'échelle fédérale, v. les Federal Rules of Civil Procedure (Fed. R. Civ. P.), rule 26(c).

228 Difficile à rendre en français dans ce contexte, le terme « sealing » signifie littéralement « scellement », c'est-à-dire le fait d'apposer un sceau. En pratique, le sealing d'un dossier aboutit à une forme d'effacement (comp. cancellation), physique (destruction) ou non (confidentialité). Dans une grande majorité de cas, l'information est simplement rendue inaccessible, sans altération physique. On parlera donc, dans les lignes qui suivent, de confidentialité.

229 V., par ex., N.Y. COMP. CODES R. & REGS. tit. 22, § 216.1 (Sealing of court records) : "(a) Except where otherwise provided by statute or rule, a court shall not enter an order in any action or proceeding sealing the court records, whether in whole or in part, except upon a written finding of good cause, which shall specify the grounds thereof. In determining whether good cause has been shown, the court shall consider the interests of the public as well as of the parties".- V. aussi, California Rules of Court, rule 2.550, (d) (Express factual findings required to seal records) : "The court may order that a record be filed under seal only if it expressly finds facts that establish : — (1)There exists an overriding interest that overcomes the right of public access to the record ; — (2)The overriding interest supports sealing the record ; — (3)A substantial probability exists that the overriding interest will be prejudiced if the record is not sealed ; — (4)The proposed sealing is narrowly tailored; and — (5)No less restrictive means exist to achieve the overriding interest".

230 Leur légalité est débattue : v. P. Winn in Judicial Conference Privacy Subcommittee.- Conference on Privacy and Internet Access to Court Files, op. cit., p. 10.

231 C'est parfois le cas en matière familiale et pour les affaires mettant en jeu des mineurs : N. Gomez-Velez, op. cit., spéc. p. 412. Concernant le cas des tribunaux pour enfants (Juvenile Courts), cf. B.C. Feld, « The Constitutional Tension Between Apprendi and McKeiver : Sentence Enhancements Based on Delinquency

28. Toutes ces règles prennent une dimension particulière à l'heure de la numérisation massive des données judiciaires et leur dépôt sur des serveurs accessibles aux citoyens depuis l'Internet. Comme on l'a bien remarqué, jusqu'à présent, l'accès à ces informations supposait de longues démarches, puisqu'il fallait se rendre auprès du greffier de la juridiction et consulter les dossiers à partir d'un nom ou d'un numéro de rôle – toutes choses qui pouvaient demander beaucoup de temps. En d'autres termes, ces informations jouissaient d'une véritable « obscurité pratique » (« *practical obscurity* »)[232]. Avec la numérisation et, surtout, la mise en ligne, cette obscurité s'évanouit à la faveur d'un accès souple et distant. Le problème se pose déjà concrètement pour les juridictions fédérales dont le *E-Government Act* de 2002[233] exige qu'elles publient en ligne, avec la listes des affaires pendantes et de celles qui ont été closes, la substance de toutes les opinions écrites rendues par la juridiction, sans égard au fait que l'opinion sera ou non publiée, et ce dans un format permettant les recherches plein-texte, de même que tous les documents produits devant la juridiction, ainsi que toute information (y inclus les formulaires dans un format pouvant être téléchargé) que la cour jugera utile pour le public. Tout citoyen peut donc désormais, grâce au service électronique d'accès public « PACER » (pour « *Public Access to Court Electronic Records* »), et moyennant la création d'un profil et le paiement de frais de consultation ($0,10 par page), accéder librement à cette immense base de données judiciaires[234].

Le législateur n'a pas été insensible aux menaces que représente PACER pour la vie privée, et la *Judicial Conference Policy on Privacy and Public Access to Electronic Case Files* a été chargée de réfléchir à l'articulation entre vie privée et transparence. Les règles applicables aux procédures civiles et pénales, aux procédures de faillite et aux procédures d'appel ont été modifiées en conséquence[235]. Dans l'ensemble, toutefois, ces règles sont jugées incomplètes et ne tiennent pas suffisamment compte de la révolution opérée par l'accès en ligne aux données judiciaires. Il est vrai que, en plus des problèmes spécifiques de sécurité[236] et de vol d'identité[237], d'atteinte possible à l'intégrité du

---

Convictions and the Quality of Justice in Juvenile Courts », 38 Wake Forest L. Rev. 1111 (2003), spéc. p. 1183, note (234).

232 J. Reindenberg in Judicial Conference Privacy Subcommittee.- Conference on Privacy and Internet Access to Court Files, « Panel One : General Discussion on Privacy and Public Access to Court Files », 79 Fordham L. Rev. 1 (2010), p. 4.

233 Pub. L. No. 107-347, § 205(a)-(b), 116 Stat. 2910, 2913-14 (codified at 44 U.S.C. §3501 (2006)).

234 Des systèmes comparables ont fait leur apparition ou devraient apparaître prochainement à l'échelle des États. Pour l'État de New-York, v. le travail de la Commission on Public Access to Court Records (Report to the Chief Judge of the State of New York, February, 2004 (http://www.nycourts.gov/ip/publicaccess/Report_PublicAccess_CourtRecords.pdf) ; pour le New Jersey : http://njcourts.judiciary.state.nj.us/web15z/ACMSPA/ ;

235 Federal Rules of Civil Procedure, règle 5.2. ; Federal Rules of Criminal Procedure, règle 49.1 ; Federal Rules of Bankruptcy Procedure règle 9037 ; Federal Rules of Appellate Procedure, règle 25.

236 Dans le domaine des violences domestiques, les informations judiciaires permettraient par exemple de localiser l'ancienne compagne : Ken Dreifach, Chief, Internet Bureau, Office of New York Attorney General to New State Commission on Public Access to Court Records 2-3 (May 30. 2003) ; et v. N. Gomez-Velez, op. cit., note (9), p. 371 ; et pour un exemple concret : v. Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005-06, (N.H. 2003).

237 Concernant le numéro de sécurité sociale, v. Crawford, 194 F.3d 954 (1999). Afin de limiter les risques de vol d'identité, la règle 5.2.(a)(1) des Federal Rules of Civil Procedure prévoit que les documents produits devant la juridiction qui contiennent un numéro de sécurité sociale, un numéro d'identification fiscale, une date de naissance, le nom d'un mineur, un numéro de compte ou une adresse personnelle, ne doivent intégrer que les cinq derniers

système judiciaire[238], l'accès en ligne provoque une perte totale de contrôle des données, fussent-elles ou non intimes (sensibles)[239] – même si, à l'heure actuelle, ces données ne sont pas indexées par les moteurs de recherche[240].

29. Ces carences sont d'autant plus regrettables que le grand texte en matière d'accès aux documents publics – le *FOIA* – a permis le développement d'une jurisprudence bien avisée des risques considérables que présente un accès largement conçu à une vaste quantité de données. Cette loi, qui date de 1966, lie fermement transparence, accès et démocratie. Lors de la signature de la loi, le Président Lydon Johnson observait emphatiquement : « Cette législation jaillit de l'un de nos principes les plus importants : une démocratie fonctionne mieux lorsque les citoyens ont accès à toutes les informations, dans la limite de la sécurité de la Nation. Nul ne devrait pouvoir jeter un voile de secret sur les décisions qui peuvent, sans dommage, être portées à l'attention du public <*decisions which can be revealed without injury to the public interest*> »[241]. Le texte ne méconnaît pourtant pas les exigences attachées à la vie privée qui prennent du reste la forme de deux exceptions pouvant être opposées aux requêtes en production de documents publics[242]. Le § 552(b) du *FOIA* précise ainsi que le texte ne s'applique pas aux : « [...] (6) fichiers personnels et médicaux et fichiers comparables dont la divulgation constituerait une atteinte manifestement injustifiée <*cleary unwarranted*> à la vie privée personnelle.— (7) dossiers et informations compilés à des fins de mise en œuvre de la loi pénale <*law enforcement purposes*>, mais seulement dans la mesure où la production de tels dossiers ou informations [...] pourrait raisonnablement conduire

---

chiffres du numéro de sécurité sociale ou du numéro d'identification fiscale, l'année de naissance, les initiales du mineur, les cinq derniers chiffres du numéro de compte et, en guise d'adresse, seulement la ville et l'État où se trouve le domicile. On trouve la même règle dans les Federal Rules of Bankruptcy Procedure (9037) et dans les Federal Rules of Criminal Procedure (49.1). Les dispositions prévues pour les procédures civile et pénale s'appliquent par renvoi à la procédure d'appel : cf. Federal Rules of Appellate Procedure (25(a)(5).- Adde, D. Solove, « Identity Theft, Privacy, and the Architecture of Vulnerability », 54 Hastings L.J. 1227 (2003), p. 1255.

238 Un large accès aux dossiers judiciaires pourrait dissuader les jurés de servir la justice ou bien affecter la sincérité des témoins : J. Reindenberg in Judicial Conference Privacy Subcommittee.- Conference on Privacy and Internet Access to Court Files, op. cit., p. 5-6. Une cour s'est prononcée contre la demande d'anonymat d'un juré : v. United States b. Blagojevich, 612 F.3d 558 (7th Cir. 2010) (opinion dissidente du juge Posner).

239 La divulgation du statut de séropositif peut être d'une gravité exceptionnelle pour l'individu (Doe v. City of New York, 15 F.3d 264 (2d Cir. 1994). Mais l'utilisation secondaire des données anodines à des fins commerciales, au moyen, par exemple, de mécanismes d'agrégations et d'exploration de données (data mining), présente des dangers qui ne doivent pas être sous-estimés. Comme indiqué en introduction, il y a va de l'autonomie décisionnelle du sujet et, plus largement, du fonctionnement normal des institutions démocratiques ; v. supra, n° 6 & 8.

240 Cf. P. Winn in Judicial Conference Privacy Subcommittee.- Conference on Privacy and Internet Access to Court Files, op. cit., p. 9.

241 2 Public Papers of the Presidents of the United States : Lyndon B. Johnson 699 (1967), cité in H.R. Rep. 104-795 (104th Cong. 2d Sess.), p. 8 (1996).

242 En vertu de cet acte, toute personne a normalement le droit d'examiner tout dossier ou document conservé par une agence fédérale, une entreprise fédérale ou un département fédéral, et d'en prendre copie. La personne publique requise doit produire des « efforts raisonnables » pour répondre à toute requête qui « décrit raisonnablement » l'information qui est recherchée. Il lui incombe de répondre dans un délai de 20 jours ouvrés. Un recours gracieux est possible pour contester tout refus (qui doit être motivé). Une fois le recours gracieux épuisé, un recours contentieux peut être introduit devant une juridiction fédérale.

à une atteinte injustifiée à la vie privée personnelle »[243]. Le texte ajoute, donnant une base possible au droit à l'oubli, que « dans la mesure nécessaire à la prévention d'une atteinte manifestement injustifiée à la vie privée personnelle, l'agence doit effacer *<delete>* les détails identifiants, lorsqu'elle rend disponible ou publie une opinion, une communication sur sa politique, une interprétation ou une instruction ou un manuel destiné aux employés »[244].

30. Soumises à la sagacité de la Cour Suprême, ces exceptions ont donné lieu à un arrêt majeur qui, s'il n'avait pas été volontairement limité par la Haute juridiction au contexte du *FOIA*[245], constituerait probablement l'une des décisions les plus importantes jamais rendues en matière de vie privée aux États-Unis. Datant de 1989, l'arrêt *United States Department of Justice v. Reporters Committee for Freedom of the Press*[246] mettait en jeu l'activité menée par le *Federal Bureau of Investigation* qui a accumulé, pendant des années, les dossiers d'antécédents criminels de plus de 24 millions de personnes, et dont la synthèse a pris le nom de « *rap sheets* ». Ces « méta-dossiers » sont très précieux pour le FIB, car ils contiennent d'innombrables informations : date de naissance, caractéristiques physiques, historique des arrestations, des accusations, des condamnations et des incarcérations du sujet. En l'occurrence, un correspondant de CBS et le *Reporters Committee for Freedom of the Press* souhaitaient pouvoir accéder au « *rap sheet* » de quatre personnes appartenant à la famille Medico, soupçonnés d'appartenir au crime organisé et d'avoir bénéficié de l'entremise d'un parlementaire corrompu pour obtenir des contrats de défense. Trois dossiers avaient été communiqués par le FBI à la suite du décès des personnes concernées. Il s'opposait en revanche toujours à la production du quatrième, se prévalant de l'exception prévue par le § 552(b)(7)(C). La divulgation de tels fichiers à un tiers pouvait, en effet, selon l'agence, « raisonnablement conduire à une atteinte injustifiée à la vie privée personnelle » (*FOIA, 5 U.S.C. § 552(b)(7)(C)*).

Si la Cour Suprême a donné raison au FBI, c'est surtout parce qu'elle a retenu une définition relativement large de la vie privée et bien perçu la menace d'une vaste collection de données publiques : « Pour commencer », indique-t-elle, « le *common law* tout comme la compréhension littérale de la vie privée incluent le contrôle, par l'individu, des informations qui concernent sa personne. Dans une société organisée, il est très peu de faits qui, à un moment ou à un autre, ne sont pas portés à la connaissance d'autrui. Ainsi l'étendue de la protection que le *common law* reconnaît au droit à la vie privée dépend, en partie, du degré de dissémination du fait privé allégué et de la mesure dans laquelle le passage du temps l'a rendu privé ». Si la Cour mentionne l'effet du temps et l'oubli qu'il rend possible, elle insiste aussi sur la nature de la divulgation. Il y a une différence à faire, insiste-t-elle, entre une « divulgation diffuse » (« *scattered disclosure* ») de « morceaux d'informations contenues dans un *rap sheet* » et la « révélation du *rap sheet* dans son ensemble ». Dans le premier cas, les informations bénéficient d'une certaine obscurité pratique puisqu'elles sont disséminées dans plusieurs dossiers situés en des lieux différents (palais de justice, archives du comté, registres des commissariats de police, etc.). Dans le second, elles

---

243 Une traduction plus littérale donnerait : « mais seulement dans la mesure où l'on pourrait raisonnablement s'attendre à ce que la production de tels dossiers ou informations cause une atteinte injustifiée à la vie privée personnelle ».

244 FOIA, § 552(a)(2).

245 V. infra, ce paragraphe.

246 United States Department of Justice v. Reporters Committee for Freedom of the Press 489 U.S. 749 (1989).

bénéficient, pour ainsi dire, d'une transparence maximale puisque, une fois numérisées, elles sont entièrement accessibles à partir d'un seul centre de gestion de l'information. Reprenant l'important *obiter dictum* de *Whalen v. Roe*, qui soulignait déjà le risque d'une vaste accumulation de données[247], elle conclut : le fait qu'« un événement ne soit pas entièrement "privé" ne signifie pas qu'un individu n'a aucun intérêt à limiter la divulgation ou la dissémination de l'information ». L'intérêt de vie privée qui réside dans un *rap sheet* est « *substantiel* » ; et « [l]e caractère substantiel de cet intérêt est affecté par le fait que, dans nos sociétés contemporaines, l'ordinateur est à même d'accumuler et de stocker des informations qui auraient été autrement oubliées bien avant que la personne [concernée] eût atteint l'âge de 80 ans [...] ». Si l'arrêt est aussi important, c'est bien parce qu'il ne se concentre pas sur la nature de l'information. En garantissant un accès facilité et centralisé à une vaste quantité de données, le *rap sheet* permet de dresser très rapidement le profil judiciaire d'un individu. Surtout, la Cour attache une importance capitale au bouleversement que l'informatique emporte à l'égard du temps et de l'oubli. Susceptible d'être rappelée dans le présent moyennant de modestes efforts, l'information est comme la flétrissure de la fleur de lys : elle marque indélébilement le sujet. Il est regrettable que la Cour Suprême ait précisé, dans une note de bas de page, que son raisonnement ne valait que pour le *FOIA*[248]. Il aurait servi de base solide à l'édification d'un droit à l'oubli en droit américain dont il faut désormais examiner les possibilités.

Section 2- Le droit à l'oubli et la vie privée personnelle

31. Lorsqu'un écrivain, un journaliste, un cinéaste ressuscite des faits anciens ou lorsqu'un journal place en ligne ses archives[249], l'oubli n'est plus en mesure d'opérer ses vertus pacificatrices. Celui dont le nom apparaît associé à un événement que la société (et l'individu lui-même parfois) avait oublié peut en subir de graves conséquences dont le droit à l'oubli serait, en Europe, le seul remède. La question s'est également posée aux États-Unis où l'on a parfois proposé le jeu du tort

---

247 V. supra, n° 20.

248 Reporters Committee, 489 U.S., p. 762, note (13). Dans un arrêt ultérieur (National Archives and Records Administration v. Favish, 541 U.S. 157 (2004)), la Cour a pareillement précisé, mentionnant l'arrêt Reporters Committee : « Nous avons observé que le droit légal [prévu par la loi, en tant que source formelle] à la vie privée, tel que garanti par l'exception 7(C), va au-delà du common law et de la Constitution. Voir Reporters Committee, 489 U.S., p. 762, n. 13 (contrastant le champ de la protection sous le FOIA avec celui des protections comparables sous le common law et la Constitution) ».

249 La question ne fera pas l'objet de développements spécifiques, car elle n'a pas encore été portée à l'attention des juridictions. Il faut toutefois mentionner cette affaire d'intérêt modeste (« small claims ») qui a reçu une certaine publicité. Elle est rapportée par un auteur dans un article récent consacré au droit à l'oubli : J.E. McNealy, « The Emerging Conflict Between Newsworthiness and the Right to be Forgotten », 39 North.Kentucky L.Rev., 119 (2012), p. 119 et s. Un footballer de l'équipe de l'Université de Berkeley avait eu maille à partir avec le personnel d'un club de strip-tease au cours d'une soirée trop arrosée. Un article du Daily Californian, journal local, avait rendu compte de ses déboires. Cinq années plus tard, après avoir définitivement l'équipe de football, le jeune homme décédait. Le père du défunt demandait au directeur en chef du journal de retirer les articles sur son fils qui étaient archivés en ligne. Face au refus, il assignait le directeur en responsabilité pour infliction of emotional distress : cf. Purtz v. Srinivasan, No. 10CESC02211 (Fresno Co. Small Cl. Ct. Jan.11,2011) ; v. le rôle, date du 26 janv. 2011 : http://banweb.co.fresno.ca.us/cprodsnp/ck_public_qry_doct.cp_dktrpt_frames?backto=P&case_id=10CESC02211&begin_date=&end_date=

de *public disclosure of private facts*. En raison, toutefois, de ses faiblesses (I), mais aussi de la toute-puissance du Premier amendement, les résultats restent nuancés (II).

I- Les faiblesses du tort de public disclosure of private facts

32. Le *Restatement (Second) of Torts* a ouvert la voie à une action en responsabilité civile au profit de celui qui a subi un dommage du fait de la divulgation d'informations personnelles. Ce *tort*, qui a été adopté dans un très grand nombre d'États[250], vient compléter les textes adoptés à l'échelle fédérale et étatique qui restreignent et sanctionnent la divulgation d'informations plus spécifiques. Dans un certain nombre d'États, par exemple, la loi interdit la révélation de l'identité des victimes d'agressions sexuelles[251] ou bien encore ouvre une action en responsabilité civile au profit de celui dont le statut de séropositif a été porté à la connaissance du public[252]. On peut véritablement parler d'une responsabilité contre le « dévoilement » de la vie privée (A) dont on verra qu'elle est entravée par l'intérêt légitime du public (B).

A- Une responsabilité contre le « dévoilement » de la vie privée

33. Selon le § 652E du *Restatement*, la responsabilité est encourue pour « [l]a révélation au public de faits qui relèvent manifestement de la vie privée d'autrui à condition que ces faits soient de nature à choquer toute personne raisonnable et qu'ils ne présentent pas d'éléments de nature à éveiller un intérêt légitime dans le public ». Le *tort* suppose la réunion de plusieurs conditions, dont l'existence de faits privés (« *private matters* »), de nature à choquer toute personne raisonnable (« *offensiveness* »), la publicité (« *publicity* ») et l'absence d'intérêt légitime du public. Au regard du droit à l'oubli, seules les première et dernière conditions méritent un examen attentif[253], et, pour la minute, il convient surtout d'étudier la première en gardant cette question à l'esprit : de quelle manière le droit américain traite-t-il la redivulgation d'informations ou la persistance d'informations sur l'Internet ?

Comme chacun l'aura compris, le présent *tort* ne peut être appliqué que lorsque les faits sont « privés ». Privilégiant une vision érémitique de la vie privée, inférant souvent du lieu de survenance du fait litigieux une forme de renonciation à la protection de la vie privée, la jurisprudence a souvent refusé d'offrir la protection du *tort* à tous ceux dont le comportement avait pu prendre place dans la sphère publique. L'arrêt *Gill v. Hearst Publishing Co.*[254], rendu par la Cour Suprême en 1953, en est une bonne illustration. Sur l'un des stands du *Farmers' Market*, à Los Angeles, deux jeunes gens s'enlaçaient langoureusement. Un photographe du *Harper's Bazaar*, qui cherchait à illustrer un reportage sur les sentiments amoureux, réalisa un cliché de la scène qui fut ensuite publié dans le magazine. Le couple se plaignit d'une atteinte à sa vie privée qui ne fut

250 Ne l'ont pas adopté les États suivants : le Nebraska, l'État de New York, la Caroline du Nord, le Dakota du Nord, l'État de Rhode Island, l'Utah et la Virginie.

251 N.Y. Civ. Rights L., § 50-b ; Pa. Comp. Stat. § 5988.

252 410 Ill. Comp. Stat. 305/9 ; Fla. Stat. § 381.004.

253 Sur la publicité, cf. Miller v. Motorola, Inc., 560 N.E.2d 900 (Ill. App. 1990).- Sur le standard des faits de nature à choquer la personne raisonnable, v. infra, n° 53 et F. Rigaux, La protection de la vie privée et des autres biens de la personnalité, op. cit., n° 628.

254 Gill v. Hearst Publishing CO., 253 P.2d. 441 (Cal. 1953).

pas reconnue par la Cour Suprême. Rappelant, à la suite de Warren et Brandeis[255], la nécessité de mettre en balance le « droit d'être laissé tranquille » avec l'intérêt public attaché à la divulgation « de faits d'actualité et d'informations en lien avec le processus démocratique », la Cour relevait surtout que, « [en] l'occurrence, les plaignants, photographiés dans leur stand soi-disant "bien connu des personnes et des voyageurs à travers le monde" pour avoir été en place pendant "des années" au sein du *Farmers' Market* "mondialement célèbre", ont volontairement exposé leur personne aux regards du public [...] ». D'où cette conclusion : « Pour autant qu'ils aient volontairement adopté cette attitude, les plaignants ont renoncé <*waived*> à leur droit à la vie privée, par leur propre action, parce qu'"Il ne peut y avoir aucune vie privée dans ce qui est déjà public." *Melvin v. Reid*, 297 P. 91, 93 »[256]. Dans le prolongement, d'autres cours ont pareillement jugé qu'apparaître en public « implique nécessairement d'ôter le voile de vie privée que la loi protège »[257]. Dans le cas de *Google Street View*, service fourni par *Google* qui permet aux internautes de naviguer virtuellement dans les rues de villes et villages, grâce à des photographies massivement prises par des véhicules équipés de caméras, une juridiction du troisième circuit a pu juger, pour repousser l'action en responsabilité d'une personne qui se plaignait de la présence de l'image de sa maison sur le site, qu'il n'était pas démontré en quoi ces faits étaient de nature à choquer une personne raisonnable[258]. Survenu en public, un fait a donc toutes chances d'être également écarté sur le fondement du standard de la personne raisonnablement sensible.

34. La jurisprudence a toutefois parfois admis que, lorsque des faits survenus en public échappaient au contrôle de l'individu et qu'il en résultait pour lui embarras ou humiliation, le *tort of public discoslure* pouvait recevoir application. Ainsi en a-t-il été jugé dans l'affaire *Daily Times Democrat v. Graham*, jugée en 1964[259]. Alors que, dans une fête foraine, une mère de famille accompagnait son fils dans une attraction appelée « Palais du rire » (« *Fun House* »), un compresseur situé sous sa robe projeta une bouffée d'air qui eut pour effet de dévoiler ses sous-vêtements. Un photographe non loin placé en profita pour saisir l'événement et l'image fut publiée quelques jours plus tard en première page d'un journal local. La juridiction n'eut aucun mal à reconnaître le caractère choquant de cette photographie pour une personne normalement sensible (retenant même la qualification d'« obscénité »). Il lui fallait, en revanche, pour retenir le *tort*, se défaire de ses précédents dont l'un, en particulier, qui énonçait que « [s]ur la voie publique, ou dans tout autre lieu public, le plaignant n'a aucun droit d'être seul »[260]. Elle y réussit finalement sans trop de peine en soulignant que « [l]orsqu'un principe juridique est poussé à l'absurde, il ne

---

255 V. supra, n° 12.

256 Sur l'affaire Melvin, v. infra, n° 44.

257 Cefalu v. Globe Newspaper Co., 391 N.E.2d 935, 939 (Mass. App. 1979).- V. également : Penwell v. Taft Broadcasting, 469 N.E.2d 1025 (Ohio App. 1984) ; un mari et sa femme étaient arrêtés dans un bar, menottés et conduit au poste de police où il était établi que l'arrestation avait été commise à la suite d'une erreur d'identité. Malheureusement pour le couple, un caméraman était présent sur le lieu de l'arrestation et ses images plus tard diffusées sur une chaîne de télévision. Se plaignant d'une atteinte à leur vie privée, les époux étaient déboutés motif pris de ce que l'arrestation avait eu lieu en public et qu'elle « avait été portée à l'attention du public ».

258 Boring v. Google, 38 Media L. Rep. 1306 (2010), non publié ; cité par D. Solove, P. Schwartz, Information Privacy Law, op. cit., p. 114.

259 Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964).

260 Forster v. Manchester, 410 Pa. 192, 189, A.2d 147.

faut pas abandonner le principe, mais éviter l'absurdité »[261] ; et de conclure : « juger que celui qui est involontairement et momentanément empêtré dans une situation embarrassante perd son droit à la vie privée simplement parce qu'il prend soudainement part à une scène publique serait contraire à la logique, faux et injuste ». Il conviendrait donc de distinguer selon que l'exposition en publique a eu lieu de manière volontaire ou qu'elle n'a été que le résultat d'un enchaînement de circonstances auquel le sujet est demeuré étranger[262].

35. Quel statut par ailleurs reconnaître aux informations qui ont déjà fait l'objet d'une *divulgation limitée* ? Sont-elles encore de nature « privée » ou ont-elles déjà intégré la sphère publique ? Le problème est consubstantiel aux réseaux sociaux lorsque les pages d'un compte sont configurées pour n'être visibles que par un nombre limité d'utilisateurs[263]. Il intéresse également les phénomènes de redivulgation et la persistance d'informations en ligne. Les juridictions sont assez souvent sensibles à l'ampleur de la divulgation et refusent de voir dans la diffusion limitée de l'information une atteinte à sa nature privée. La décision la plus importante sous ce regard a été rendue dans l'affaire *Times Mirror Co. v. Superior Court*[264]. Le demandeur, Doe (le pseudonyme couramment utilisé par les juridictions lorsque la partie bénéficie de l'anonymat), avait découvert le corps sans vie de son colocataire dans l'appartement qu'il occupait avec lui et avait pu entrevoir celui qui avait tout lieu d'être son meurtrier. Ce dernier n'ayant pas encore été arrêté, la police avait choisi de dissimuler l'identité de ce témoin-clé. Un journal finit toujours par en avoir connaissance et divulgua l'information à l'occasion d'un article consacré à l'affaire. Doe introduisit une action en responsabilité contre le journal pour *disclosure of truthful information* et le journal fit valoir, en réplique, que l'information n'était plus privée ayant été divulguée par le demandeur à des voisins, des amis, des membres de sa famille, ainsi qu'à des policiers. Pour la cour, toutefois, Doe n'avait pas « rendu l'information, par ailleurs privée, publique en coopérant avec la police et en cherchant du réconfort auprès de ses amis et de ses proches ». Dans une autre affaire[265], un couple souhaitant recourir à la fécondation *in vitro*. Les époux étaient très attachés à la non-divulgation de l'information, car l'assistance médicale à la procréation à laquelle ils entendaient recourir était condamnée par la confession à laquelle ils appartenaient. En dépit de leurs efforts, ils furent filmés par un caméraman de la télévision qui assistait à une fête organisée au profit de ces couples recourant à la procréation médicalement assistée. Pour la cour, les demandeurs avaient conservé une *espérance de vie privée*, parce qu'en « assistant à ce rassemblement limité [...] ils n'avaient pas renoncé à ce que leur situation et leur recours à la fécondation restent privés ». Une solution comparable a été retenue dans une affaire impliquant une personne

---

261 Hinish v. Meir & Franck Co., Inc., 113 P.2d 438.

262 Mais voir, toutefois : NcMamara v. Freedom Newspapers, Inc., 802 S.W. 2d 901 (Tex. Ct. App. 1991), à propos d'un lycéen qui, au cours d'un match de football, dévoile par inadvertance ses parties génitales. Un journal publiait plus tard les images, ce dont se plaignait le lycéen. Pour la cour, qui rejette la demande, le précédent Graham ne méritait pas d'être appliqué (on notera que la Cour attache une certaine importance au fait – pourtant très peu probable – que personne n'avait relevé, au cours du processus de publication, que les parties génitales de l'adolescent était exposées).

263 Sur cette question non développée dans ces lignes, cf. L.J. Strahilevitz, « A Social Networks Theory of Privacy », 72 U. Ch. L. Rev. 919 (2005).

264 Times Mirror Co. v. Superior Court, 244 Cal. Rptr. 556 (Cal. Ct. App. 1988).

265 Y.G. v. Jewish Hospital, 795 S.W.2d 488 (Mo. Ct. App. 1990).

séropositive qui avait révélé sa maladie à environ une soixantaine de personnes (membres de la famille, amis, médecins et membres d'un groupe de soutien), circonstance jugée insuffisante, selon la cour, pour faire disparaître le caractère privé de l'information[266].

Mais, comme l'indiquent Daniel Solove et Paul Schwartz[267], cette jurisprudence est loin d'être homogène. Dans une affaire[268] d'une particulière gravité, une magistrate colombienne, qui avait poursuivi le baron de la drogue, Pablo Escobar, avait été contrainte, après avoir reçu des menaces de mort, de démissionner et de se réfugier à Détroit où elle avait été nommée en qualité de consul. Quelques personnes furent informées de sa véritable identité : les autres consuls, bien sûr, qui reçurent l'information par courrier. En quelques occasions, la demanderesse n'avait du reste pas hésité à utiliser sa carte professionnelle portant son nom ; le bail de son appartement mentionnait son identité et quelques voisins connaissaient son ancienne activité de magistrate. Quand des journalistiques portèrent l'affaire à la connaissance du public, révélant au passage son adresse, le consul agit en responsabilité, notamment pour divulgation de faits privés. Pour la cour, qui vint ainsi confirmer la décision des premiers juges, l'identité de la demanderesse « aux États-Unis était accessible au public ». Dans l'affaire *In Fisher v. Ohio Dep't of Rehabilitation and Correction*[269], enfin, une Cour a pareillement pu juger que le partage d'informations sensibles avec quatre co-employés était suffisant pour faire disparaître toute espérance de vie privée dans ces informations.

36. Il est difficile de tracer une ligne ferme entre ces deux séries de précédents. Le nombre de personnes en possession de l'information n'est pas un critère opérationnel. Une confession faite à quatre collègues a suffi, selon l'opinion d'une cour, à faire disparaître la nature privée de l'information (*Fisher*), là où, dans un autre arrêt, la divulgation du statut de séropositif à soixante personnes n'a pas été jugée suffisante (*Duran*). Faut-il alors tenir compte de la nature de l'information (*l'identité* dans une affaire faisant pesant un risque sur la sécurité d'une personne, l'état de *santé* et en particulier le statut de séropositif) et la cohérence du groupe, les normes (pratique, usages) qui sont observées en son sein, notamment du point de vue de la circulation de l'information ? C'est ce que l'on a suggéré[270] et il faudra y revenir en examinant la question des contrats implicites de confidentialité[271].

37. Toutes ces questions restent essentielles du point de vue du droit à l'oubli. Les faits (très souvent personnels) dont s'alimente la presse, le cinéma ou le monde du livre surviennent généralement en public ou entrent dans la sphère publique à l'occasion d'une action en justice. N'étant plus privées, ils ne bénéficient ainsi normalement plus de la protection du *tort of disclosure of truthful information*. Mais là encore, rien n'empêche de s'interroger, à l'instar de quelques juridictions françaises, sur le possible effet du temps. N'est-il pas possible d'admettre que, passé un certain temps, les faits soient revenus à la sphère privée ? Étant apparemment sortis du

---

266 Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491 (Ga. 1994).

267 D. Solove, P. Schwartz, Information Privacy Law, op. cit., p. 118.

268 Duran v. Detroit News, Inc., 504 N.W.2d 715 (Mich. Ct. App. 1993).

269 In Fisher v. Ohio Dep't of Rehabilitation and Correction, 578 N.E.2d 901 (Ohio Ct. Cl. 1988).

270 Cf. L.J. Strahilevitz, art. préc.

271 V. infra, n° 48.

contexte brûlant qui les a vus naître et qui avait, en son temps, justifié l'attention du public, plus rien ne paraît faire obstacle à leur oubli. Quant à la question de la divulgation limitée de l'information, elle rappelle que des précautions sont parfois prises *ab initio* pour éviter la propagation de l'information. L'identité d'un témoin est gardée confidentielle, des informations sensibles sont soigneusement conservées au sein d'un cercle de proches... Il est pourtant rare, surtout lorsque l'information présente une dimension publique, que le secret soit gardé bien longtemps. Et la presse, dont c'est le métier et parfois le rôle, opère comme une immense caisse de résonnance. Les faits, dira-t-on, étaient certes privés (du moins à certaines conditions) ; mais bénéficient-ils pour autant du *tort of disclosure* ? Rien n'est moins sûr. Le contexte de ces divulgations, qui met souvent aux prises un citoyen et la presse, laisse présumer l'intérêt public dans la divulgation (pour ne rien dire de l'inexpugnable liberté d'expression).

En définitive, ces deux séries de difficultés, qui ne sont pas tout à fait comparables, doivent être examinées à travers le même prisme, celui de l'intérêt légitime du public. Cette condition, également appelée *newsworthiness test*, permet de pénétrer dans l'antichambre de la liberté d'expression.

B-Une responsabilité entravée par l'intérêt légitime du public

38. Même lorsqu'il est établi que les faits portés à la connaissance du public relevaient manifestement de la vie privée d'autrui, la responsabilité peut être écartée dès lors qu'ils présentaient des éléments de nature à éveiller un intérêt légitime dans le public. Dans l'affaire *Duran* précitée[272], la Cour, après avoir estimé que l'information litigieuse « était accessible au public », relevait : « Bien que la divulgation de l'adresse [de la demanderesse] puisse être regardée comme hautement critiquable dans ces circonstances, l'information était d'un intérêt légitime pour le public en raison du danger que faisaient courir à [ses] voisins les menaces de mort [adressées à la demanderesse] ». L'intérêt légitime du public est un moyen de défense efficace[273] au service des entreprises de presse et des maisons d'édition qui peuvent ainsi démontrer que, d'après les « coutumes et conventions de la communauté », d'après ses « mœurs », l'information méritait d'être divulguée[274]. Ce qui est particulièrement troublant, c'est que l'examen de cette condition conduit en réalité les juges en mettre en balance la vie privée et la liberté d'expression (et de la presse), comme s'ils examinaient la conformité d'une disposition législative au Premier amendement de la Constitution. Solove et Schwartz expliquent que « [b]eaucoup d'affaires appliquant le test de l'intérêt légitime du public <*newsworthy test*> procèdent ainsi de manière à éviter les difficultés soulevées par le Premier amendement ». Mais ils rappellent que les

---

272 Duran v. Detroit News, Inc., 504 N.W.2d 715 (Mich. Ct. App. 1993).

273 G. Dendy, « The Newsworthiness Defense to the Public Disclosure Tort », 85 Ky. L.J. 147 (1997).

274 Restatement (Second) of Torts § 652D (1977), § 652D Publicity Given to Private Life, Comment on Clause b), h (Westlaw). Le commentaire officiel indique également que « la ligne doit être tracée là où la publicité ne correspond plus à la divulgation d'informations à laquelle le public a droit, et devient, purement et simplement, une immixtion malsaine et sensationnelle dans la vie privée d'autrui et dont une personne raisonnablement décente dirait qu'elle est sans intérêt ».- V. aussi, D. Solove, P. Schwartz, Information Privacy Law, op. cit., p. 128.

« [a]pplications du *tort* – impliquant peut-être même des faits qui ne méritent pas de faire l'actualité – sont toujours justiciables d'une contestation autonome sur le fondement du I^er^ amendement »[275]. Les juridictions contournent parfois la difficulté en examinant le critère de l'intérêt légitime du public à la lueur du Premier amendement, réunissant ainsi, dans un même contrôle, les exigences du *common law* et du droit constitutionnel[276]. En tout état de cause, ainsi qu'on s'en rendra compte, les résultats du contrôle opéré dans le cadre du *tort* aboutissent souvent aux mêmes résultats que ceux obtenus dans le domaine constitutionnel, même si le raisonnement n'est pas toujours semblable.

39. Parmi les situations archétypales qui alimentent le débat passé et actuel sur le droit à l'oubli figurent le cas de ces personnalités anonymes qui, à la faveur d'un événement provoquant une certaine émotion ou s'inscrivant simplement hors du cours normal des choses, se trouvent soudain placées sous le regard du public. Le droit américain les désigne sous le nom de personnages publics involontaires (« *involuntary public figures* »)[277]. Ils partagent un sort commun avec les personnages publics véritables (« *voluntary public figures* ») (hommes politiques, comédiens, artistes, sportifs célèbres, etc.), à cette différence près, toutefois, que leur trajectoire individuelle ne croise souvent celle de l'histoire que de manière *fugace*, c'est-à-dire sans laisser de trace durable. La mémoire est naturellement portée à les oublier à mesure que s'émousse la tranchante actualité de l'événement qui les a portés à la lumière. Le *Restatement (Second) of Tort* le reconnaît dans l'un de ses commentaires, même si c'est avec force réserves :

> « Le fait qu'un certain laps de temps, fût-il particulièrement long, se soit écoulé, depuis l'événement qui a fait du demandeur un personnage public, ne tient pas en échec le droit d'en faire la publicité ou d'en renouveler la publicité lorsqu'il a déjà été publié. Les événements et faits passés peuvent de nouveau rencontrer l'intérêt légitime du public, et le rappel à la vie mémorielle de ce qui est survenu plusieurs années auparavant peut être à la fois intéressant et utile à des fins d'information et d'éducation. Un tel laps de temps est, toutefois, un facteur à prendre en compte, avec d'autres faits, afin de déterminer si la publicité ne va pas trop loin dans la révélation des faits sur celui qui a souhaité retrouver cette vie confidentielle et rangée que mène la grande majorité de la communauté <*one who has resumed the private, lawful and unexciting life led by the great bulk of the community*> »[278].

---

275 D. Solove, P. Schwartz, op. cit., p. 128.- V. aussi les remarques de Lior Strahilevitz, « Reunifying Privacy Law », 98 Cal. L. Rev. 2007 (2010), spéc. p. 2033 qui juge l'application du newsworthy test superflu et plaide pour une application du seul Premier amendement.

276 V., en particulier, Shulman v. Group W Productions, Inc. 955 P.2. 469 (Cal. 1998) : « Although we speak of the lack of newsworthiness as an element of the private facts tort, newsworthiness is at the same time a constitutional defense to, or privilege against, liability for publication of truthful information [...]. Indeed, the danger of interference with constitutionally protected press freedom has been and remains an ever-present consideration for courts and commentators struggling to set the tort's parameters, and the requirements of tort law and the Constitution have generally been assumed to be congruent [...]. Little is to be gained, therefore, in attempting to keep rigorously separate the tort and constitutional issues as regards newsworthiness, and we have not attempted to do so here ».

277 Cf. Restatement (Second) of Torts § 652D (1977), § 652D Publicity Given to Private Life, Comment on Clause h).

278 Restatement (Second) of Torts § 652D (1977), § 652D Publicity Given to Private Life, Comment on Clause k).

40. Peut-être en partie à cause de ces nuances, de ce conflit apparent entre oubli et intérêt légitime du public, la vie privée n'est, jusqu'à présent, jamais sortie triomphante. L'affaire *Haynes v. Alfred A. Knopf, Inc.*[279] donne à voir la prévention des juridictions lorsqu'il s'agit de reconnaître une forme de droit à l'oubli. En l'occurrence, l'éditeur Alfred A. Knopf, Inc. publiait, en 1991, l'ouvrage historique de Nicholas Lemman intitulé « *The Promised Land : The Great Black Migration and How It Changed America* »[280]. Dans ce livre, qui connut un grand succès commercial, Lemman décrivait la migration des populations Afro-Américaines des zones rurales du sud vers les zones urbaines du nord des États-Unis, entre 1940 et 1970. La description s'articulait principalement autour du récit des heurs et malheurs d'un individu : Luther Haynes. Après un premier mariage chaotique, qu'il avait lui-même compromis par son alcoolisme et son intempérance, Luther se remaria et mena une vie tranquille. Nul, dans sa nouvelle communauté, ne connaissait son passé, en particulier l'attitude parfois violente qu'il avait pu avoir à l'endroit de son ancienne épouse. Devenu diacre de son église, percevant, avec son épouse, des revenus confortables, la lumière crue jetée sur son passé trouble était susceptible de porter une grave atteinte à son honneur et sa réputation. Il assigna donc l'auteur et son éditeur en responsabilité sur le fondement du *tort of public disclosure*. Le juge Posner devait rejeter la demande aux motifs suivants :

> « Les deux critères, le caractère choquant <*offensiveness*> et d'actualité <*newsworthiness*>, sont liés. Un individu [...] est beaucoup plus choqué par la publication de faits personnels intimes lorsque la communauté n'y trouve pas d'autre intérêt que de ressentir le frisson voyeuriste qui accompagne le franchissement du mur de vie privée qui entoure un inconnu. Le lecteur d'un livre sur la migration afro-américaine vers le nord n'aurait aucun intérêt légitime dans les détails portant sur la vie sexuelle de Luther Haynes ; mais aucun détail de cette nature n'est divulgué. Un tel lecteur a, en revanche, un intérêt légitime dans les aspects du comportement de Luther que le livre révèle [...]. Tous les détails du livre dont il est prétendu qu'ils envahissent la vie privée de Haynes sont pertinents au regard de l'histoire que l'auteur souhaitait raconter, une histoire qui n'est pas seulement d'un intérêt public légitime mais transcendant ».

Un peu avant dans son opinion, le juge Posner relevait que, « quoiqu'il puisse être douloureux pour les Haynes de voir un passé qu'ils auraient plutôt souhaité oublier porté à l'attention du public, le public a besoin de l'information communiquée par le livre, dont l'information sur Luther et Dorothy Haynes, de manière à évaluer les questions politiques et sociales profondes soulevées par l'ouvrage ».

41. On ne reprochera pas au juge Posner de ne pas prendre le travail de recherche au sérieux – travail qui pourrait d'ailleurs se réclamer, en l'occurrence, des droits de l'histoire. Pratiquant une sorte de microhistoire, suivant le chemin d'un destin particulier pour retrouver les grandes routes de l'Amérique, il était inévitable que Lemman divulgue des faits privés – et le juge

---

279 Haynes v. Alfred A. Knopf, Inc., 8F.3d 1222 (7th Cir. 1993).

280 N. Lemann, The promised land : the great Black migration and how it changed America, A.A. Knopf, New York, 1991 (non traduit en français).

respecte pleinement la méthodologie[281]. L'intérêt du public dans un aspect de l'histoire des États-Unis n'est pas contestable et la préséance donnée à la libre communication des idées sur la vie privée et l'oubli se comprend parfaitement dans un système juridique qui accorde une telle valeur constitutive à la liberté d'expression. On ne peut toutefois rester parfaitement insensible au sort du demandeur dont la vie s'est probablement trouvée bouleversée et qui a dû remettre à plus tard sa rédemption. Comme les défenseurs de la vie privée l'ont souligné[282], un meilleur équilibre entre les deux intérêts peut parfois être obtenu en empêchant tout simplement la divulgation des informations identifiantes. Dans l'affaire *Barber v. Time, Inc.*[283], par exemple, le célèbre hebdomadaire américain, qui avait consacré un article à la maladie singulière d'une patiente, se voyait reprocher d'avoir publié la photographie de la demanderesse sur son lit d'hôpital. Pour la juridiction, en effet, « tandis que la maladie de la demanderesse, parce qu'inhabituelle, était peut-être une question d'intérêt public, l'identité de la personne souffrant de cette maladie ne l'était certainement pas »[284].

Sous ce regard, l'affaire *Haynes* présente peut-être, il est vrai, une particularité soulignée par le juge Posner : en renonçant à dévoiler l'identité de Haynes, Lemann aurait dû, par là même, renoncer à son essai historique et rédiger une œuvre de fiction ; et « l'étude non quantitative de personnes vivantes, serait abolie en tant que catégorie de recherche, pour être remplacée par le roman social ». Par ailleurs, même en changeant les noms, note Richer Posner, « [l]es détails de la vie des Haynes relatés dans le livre auraient permis à quiconque les connaissant bien depuis longtemps [...] ou les ayant connus avant leur mariage, de les identifier ». Si l'analyse est exacte, elle ne tient cependant pas suffisamment compte du bouleversement introduit par l'Internet. Dans le domaine des publications papier, la présence ou l'absence du nom ne change sans doute pas grand-chose. La distinction devient en revanche cruciale sur l'Internet où il est si simple de recoller un grand nombre d'informations à partir d'un nom, informations du reste appelées à ne plus disparaître. Mais confessons-le, ces remarques restent très éloignées des considérations des juridictions américaines pour lesquelles *l'identité en tant que telle* constitue une information d'un intérêt légitime pour le public. C'est qu'il y va, soulignent-elles souvent, de l' « impact ou de la crédibilité » de l'écrit vecteur de la divulgation[285] ; parce que la révélation de l'identité « permet au public de percevoir avec une plus grande acuité les mérites de la controverses »[286] ou de mesurer la « crédibilité et la force persuasive du récit »[287]. L'information du public a ses exigences que le

---

281 Haynes, op. cit., § 29 : « Lemann's book has been praised to the skies by distinguished scholars, among them black scholars covering a large portion of the ideological spectrum – Henry Louis Gates Jr., William Julius Wilson, and Patricia Williams. Lemann's methodology places the individual case history at center stage. If he cannot tell the story of Ruby Daniels without waivers from every person who she thinks did her wrong, he cannot write this book ».

282 V., en particulier, D. Solove, « The Virtues of Knowing Less : Justifying Privacy Protections Against Disclosure », 53 Duke L.J. 697 (2003), spec. p. 1018-1019.

283 Barber v. Time, Inc., 159 S.W. 291 (Mo. 1942).

284 Cité par D. Solove, P. Schwartz, op. cit., p. 132.

285 Gilbert v. Medical Economics Co., 665 F.2d 305 (10th Cir. 1981).

286 Howard v. Des Moines Register & Tribune Co., 870 F.2d 271 (5th Cir. 1989).

287 Ross. v. Midwest Communications, Inc., 870 F.2d 271 (5th Cir. 1989).- Sur ces trois arrêts, v. D. Solove, P. Schwartz, Information Privacy Law, op. cit., p. 133-134.- V. aussi, sur cette question : D.L. Zimmerman, « Requiem for a Heavyweight : A Farewell to Warren and Brandeis's Privacy Tort », 68 Cornell L. Rev. 291 (1983), spéc. p. 356 ;

Premier amendement, mieux que n'importe quelle autre disposition, a su défendre contre les assauts de la vie privée et du droit à l'oubli.

II- La toute-puissance du premier amendement

42. C'est pour limiter les excès de la liberté de la presse et de la liberté d'expression que Warren et Brandeis ont plaidé pour le développement du « droit d'être laissé seul »[288]. Comme ils l'énoncent en un endroit : « La presse outrepasse de toutes parts les limites évidentes de la correction et de la décence. Le commérage n'est plus réservé au désœuvré et au vicieux, c'est devenu une industrie effrontément exercée »[289]. Depuis sa naissance, le droit à la vie privée entretient donc, aux États-Unis, des rapports complexes avec le Premier amendement. Brandeis, à qui la vie privée doit tant, a lui-même contribué à les rendre plus prégnants encore en portant au pinacle la liberté d'expression dans son opinion concordante sous *Whitney v. California* : « Croyant dans le pouvoir de la raison qui s'exerce par le débat public, ils [les Pères Fondateurs] ont évité le silence imposé par la loi – l'argument de force dans sa pire forme. Reconnaissait les possibles tyrannies de la majorité au pouvoir, ils ont amendé la Constitution de manière à ce que soit garantie la liberté d'expression et de réunion »[290]. Cet éloge du libre discours a une première conséquence qu'il n'est pas difficile de percevoir : c'est la mise à l'écart de la vie privée (1). En certaines hypothèses, toutefois, l'éloge du libre discours est de nature à offrir une meilleure protection à la vie privée (2).

A- Éloge du libre discours : la mise à l'écart de la vie privée

43. Peut-être faut-il indiquer d'ores et déjà dans quel contexte l'exception de constitutionnalité est appelée à se présenter devant les juridictions. Le *tort of public disclosure* met évidemment aux prises des parties privées, bien souvent un particulier qui se plaint d'une atteinte portée à sa vie privée et la presse qui revendique le droit de pouvoir s'exprimer librement sur tout sujet intéressant le public. Le litige étant horizontal, la Constitution ne s'applique normalement pas. Mais les moyens de l'État étant mobilisés – ses juridictions, sa force publique, etc. –, se pose finalement une question de compatibilité entre l'intervention de l'État, dont les représentants peuvent éventuellement prononcer des sanctions contre la presse, et la liberté d'expression[291]. Disons-le aussi d'emblée, certaines catégories de discours ne sont pas protégées. Tel est le cas, notamment, de l'obscénité[292], la pornographie infantile[293], la diffamation au sens strict[294], la fraude[295], le parjure[296] ou l'incitation à une action illégale imminente[297]. Il convient également

---

E. Volokh, « Freedom of Speech and Information Privacy : The Troubling Implications of a Right to Stop People from Speaking About you », 52 Stan. L. Rev. 1049 (2000), spéc. p. 1093.

288 S.D. Warren, L.D. Brandeis, « The Right to Privacy », Harvard Law Review, vol. 4 (1890), p. 193-220.

289 S.D. Warren, L.D. Brandeis, « Le droit à la vie privée (1890) », in Clio@Themis n° 3, n° 5.

290 Brandeis, J., « opinion concordante » in Whitney v. California, 274 U.S. 357, 47 S.Ct. 641, 71 L.Ed. 1095 (1927).

291 D. Solove, P. Schwartz, Information Privacy Law, op. cit., p. 147.

292 Roth v. U.S., 354 U.S. 476, 483, 77 S. Ct. 1304, 1 L. Ed. 2d 1498 (1957).

293 New York v. Ferber, 458 U.S. 747, 102 S. Ct. 3348, 73 L. Ed. 2d 1113 (1982).

294 New York Times Co. v. Sullivan, 376 U.S. 254, 84 S. Ct. 710, 11 L. Ed. 2d 686 (1964).

295 Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 771, 96 S. Ct. 1817, 48 L. Ed. 2d 346 (1976).

d'ajouter que la Cour Suprême exerce généralement un contrôle strict ou intermédiaire[298] sur les dispositions qui limitent la liberté d'expression, et elle peut encore moduler son contrôle selon qu'il est fondé sur le contenu du discours (« *Content Based* »)[299] ou non (« *Content-Neutral Regulation* »)[300]. Par le jeu de cette dernière règle, une catégorie non protégée de discours peut aussi bien bénéficier d'un contrôle étroit sous le Premier amendement s'il est établi que la loi, en interdisant, en particulier, tel ou tel contenu, a créé une discrimination qui est sans rapport avec les motifs profonds qui ont conduit à exclure *in globo* une catégorie de discours. Tel serait le cas d'une loi qui ne condamnerait la diffamation que lorsque les propos seraient dirigés contre le Gouvernement[301].

44. Le cadre d'analyse étant posée, il faut désormais montrer comment s'articulent concrètement liberté d'expression et droit à la vie privée et s'efforcer d'évaluer si un droit à l'oubli est possible en droit américain. Deux arrêts, en particulier, méritent un examen attentif, car les faits ressemblent beaucoup à ceux des affaires Landru et Mesrine[302].

La première affaire est celle dite du « Kimono Rouge », qui date de 1931, rendue par la *Court of Appeal* de Californie[303]. Gabrielle Melvin avait eu une jeunesse mouvementée. Prostituée, évoluant dans le monde de la pègre, elle avait été accusée à tort d'un meurtre en 1918. La presse s'était emparée de cette affaire qui avait fait grand bruit. Acquittée, elle se rangea et mena une vie paisible[304]... au moins jusqu'en 1930, date à laquelle elle prit connaissance de l'existence d'un film, « Le Kimono Rouge », relatant les épisodes de sa vie passée, sous son nom de jeune fille : Gabrielle Darley. Elle chercha à obtenir en justice des dommages intérêts du producteur du film, à qui elle reprochait d'avoir brisé sa vie en faisant d'elle la proie de la médisance et de la méchanceté de son entourage qui ignorait tout de son ancienne vie. La cause n'était pas simple, car les faits avaient été consignés dans le dossier judiciaire, accessible à tout citoyen. La cour se fonda plutôt sur le fait qu'on avait utilisé son nom véritable sans que cela fût véritablement nécessaire et qu'on s'immisçait ainsi sans droit dans son intimité et sa vie privée. Mais il lui fallait encore trouver un fondement, à une époque où la Californie ne disposait d'aucune loi érigeant en *tort* les atteintes portées à la vie privée par *public disclosure*. La Court of Appeal eut l'habileté de recourir à l'article 1er de la Constitution, qui ne contenait pas encore de référence expresse à la vie

---

296 18 U.S.C.A. § 1621 ; et v. In re Michael, 326 U.S. 224, 227, 66 S. Ct. 78, 90 L. Ed. 30 (1945).

297 Brandenburg v. Ohio, 395 U.S. 444, 447--449, 89 S. Ct. 1827, 23 L. Ed. 2d 430 (1969) (per curiam).

298 V. supra, n° 21.

299 Tombe sous cette catégorie un texte qui réprime l'incitation à la haine et à la violence (« fighting words ») fondée sur l' « appartenance ethnique <race>, la couleur, les croyances <creed>, la religion ou le sexe » (R.A.V. v. City of St. Paul, 505 U.S. 377 (1992)).

300 Entrent dans cette catégorie les lois qui ne réglementent que le temps, le lieu et le mode d'expression du discours, sans égard à son contenu : D. Solove, P. Schwartz, op. cit., p. 148.

301 Cf. R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).

302 Sur lesquels, v. supra, n° 4.

303 Melvin v. Reid, 297 P. 91 (Cal. Ct. App. 1931).

304 Cette vision idyllique de la réhabilitation de Melvin a été contestée : L.M. Friedman, Guarding Life's Dark Secrets : Legal and Social Controls over Reputation, Propriety, and Privacy, Stanford University Press, Stanford, 2007, spéc. p. 216-218.

privée[305], mais qui garantissait toutefois de manière large, aux citoyens, le « droit au bonheur », en l'occurrence perdu par Gabrielle Melvin[306]. Elle jugea ainsi, à propos du droit au bonheur : « Ce droit, par sa nature même, inclut le droit de vivre à l'abri des attaques injustifiées portées par autrui à sa liberté, sa propriété et sa réputation. Toute personne vivant avec droiture a droit au bonheur qui comprend la liberté contre les attaques injustifiées portées contre son caractère, son statut social ou sa réputation ». La référence à l'oubli et à la rémission des fautes apparaît plus nettement lorsque la cour énonce que :

> « [l]'un des objectifs majeurs de la société, telle qu'elle est désormais constituée, ainsi que de l'administration de notre justice pénale, est la réhabilitation du déchu et l'amendement du criminel. En vertu de ces théories sociologiques, il est de notre mission que de relever et de soutenir le malheureux, plutôt que de le tirer vers le bas. Lorsque, par ses propres efforts, une personne a réussi à se réinsérer, nous devons, nous les bien-pensants de la société, lui permettre de poursuivre dans la voie de la rectitude plutôt que de la jeter de nouveau dans une vie de honte et de crime. Même le voleur sur la croix a eu le droit de se repentir pendant les heures de son agonie finale ».

Or, en utilisant son véritable nom, le producteur avait empêché tant la réinsertion que le repentir de Melvin.

45. Si l'arrêt *Melvin* offre de solides fondements au droit à l'oubli (*droit au pardon, droit de se réinsérer*), il présente la grande faiblesse d'être peu disert concernant l'articulation entre la vie privée et le Premier amendement. On ne peut faire le même reproche à l'autre affaire, *Briscoe v. Reader's Digest Association, Inc.*, jugée en 1971 par la Cour Suprême de Californie[307]. Marvin Brisco était un voleur de camions repenti. Le *Reader's Digest*, qui consacrait un dossier à ce genre d'infractions, relatait au détour de l'article un vol particulièrement violent auquel Briscoe avait pris part quelques années plus tôt ; il y était nommément désigné. Briscoe poursuivit le *Reader's Digest*. Tout comme Melvin dans l'affaire précédente, il se disait lui aussi assagi et la publication de l'article mentionnant son nom lui causait un tort considérable. Le *complaint* indique d'ailleurs que sa fille de onze ans avait depuis lors renoncé à lui adresser la parole. Les premiers juges avaient déclaré la demande irrecevable, faute d'intérêt suffisant (« *failure to state a claim or a cause of action* »). C'est cette question de recevabilité qui est examinée par la Cour Suprême de Californie. Elle attache cette fois-ci une grande importance au Premier amendement dont le but, énonce-t-elle, est « "d'offrir, à chaque membre du corps politique exerçant son droit de vote, la plus grande participation possible dans l'appréhension de ces problèmes avec lesquelles les citoyens d'une société autonome doivent composer" *A. Meiklejohn, Political ***870 ***38 Freedom: The Constitutional Powers of the People (1960) p. 75* ». Et pour la Cour, il ne fait aucun doute que les comptes rendus d'activités délictuelles ou criminelles récentes ressortissent au « domaine légitime de la liberté de la presse ». Les circonstances dans lesquelles l'infraction a été commise, les

---

305 V., désormais, supra, n° 17.

306 Le texte était ainsi rédigé : « All men are by nature free and independent, and have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety and happiness ».

307 Briscoe v. Reader's Digest Association, Inc. (483 P.2d34 (Cal. 1971)).

techniques utilisées par les délinquants ou criminels, ainsi que la tragédie qui a frappé les victimes, voilà autant de « petits bouts vitaux d'informations » dont les citoyens ont besoin[308]. Le Premier amendement ne s'oppose donc pas à ce qu'un compte rendu fidèle d'infractions récentes, assorti du nom du suspect ou de l'auteur de l'infraction, soit publié.

Reste que, pour la Cour Suprême de Californie, les faits imposent qu'il soit *distingué*. Il était ici question de crimes passés (« *Past crimes* »), d'auteurs d'infractions anciennes (« *Past offenders* »). Si, pour la juridiction, il ne fait aucun doute que des infractions anciennes puissent faire l'actualité (« *newsworthy* »), leur relation pouvant avoir du reste les mêmes vertus que celles attachées aux comptes rendus d'infractions récentes, il n'en demeure pas moins que « l'identification du Sujet dans les comptes rendus d'infractions vieilles de plusieurs années ne présente aucune utilité publique spécifique. Une fois que les poursuites judiciaires ont pris fin, et que le suspect ou l'auteur de l'infraction a été libéré, l'identité de l'individu n'apporte généralement rien à l'administration de la justice ». Reprenant ensuite le commentaire k) du *Restatement (Second) of Torts*, celui suggérant la prise en compte de l'effet du temps sur l'appréciation de l'intérêt légitime du public (« *newsworthiness* »), la Haute juridiction relève de manière déterminante que « [l]orsqu' un homme a retrouvé "cette vie confidentielle et rangée" que mène [la grande majorité de la communauté], le *Restatement* donne à entendre qu'il n'a plus besoin de "satisfaire la curiosité du public" ». L'invocation du précédent *Melvin* renforce encore l'effet reconnu au temps et à l'oubli : *c'est qu'ils assurent l'intégrité du processus de réinsertion*. En particulier, note la Cour, « [l]'une des prémisses du processus de réinsertion, est que le délinquant réhabilité puisse rejoindre la plus grande partie de la communauté qui l'avait ostracisé pour ses actes antisociaux. Étant devenu un « homme nouveau », il a le droit, en contrepartie, de se dissimuler dans la pénombre ». Même si la liberté d'expression peut se réclamer du puissant Premier amendement, on ne saurait pour autant tenir la vie privée pour abrogée. Le passage du temps peut s'opposer à la redivulgation d'un fait porté à la connaissance du public, en particulier lorsqu'il n'est pas nettement démontré en quoi cette redivulgation sert l'intérêt légitime du public. Une subtile mise en balance des intérêts en jeu doit parfois aboutir à faire triompher la vie privée et à reconnaître une forme de droit à l'oubli :

> « Ce serait faire usage d'une fiction juridique grossière d'alléguer que dès lors qu'une question est devenue publique elle ne peut plus jamais redevenir privée. L'oubli humain qui s'opère au fil du temps fait des "toute dernières" actualités <*"hot" news*> d'aujourd'hui les archives poussiéreuses de demain. Dans une nation de 200 millions de personnes, chacun a l'occasion, même celui qui a mauvaise réputation <*the infamous*>, de commencer une nouvelle vie ».

---

308 Sans compter que ces comptes rendus peuvent, selon la Cour, servir à défendre les valeurs desservies par la garantie constitutionnelle d'un droit procès équitable. Même si une affaire ne doit pas être « jugée dans les journaux », les comptes rendus d'un crime ou d'une procédure pénale peuvent encourager les témoins encore inconnus à venir livrer leur témoignage utile et les amis ou parents à venir en aide à la victime.

46. Très sévèrement critiqués par les défenseurs de la liberté d'expression[309] – qui forment du reste aujourd'hui la très grande majorité de la doctrine étasunienne – ces arrêts ne représentent plus l'état du droit américain. Une juridiction, en particulier, a bien exprimé le point de vue de cette doctrine attachée à la toute-puissance du Premier amendement : « la jurisprudence Melvin, paternaliste en ce qu'elle doute de l'aptitude des personnes à accorder un poids raisonnable plutôt qu'excessif aux antécédents criminels d'une personne, est morte »[310]. Il faut dire que plusieurs arrêts de la Cour Suprême ont rappelé avec force la puissance de la liberté d'expression et de la liberté de la presse auxquelles l'État ne saurait apporter de restrictions qu'avec la plus infinie réserve. Le premier arrêt – *Cox Broadcasting Corp v. Cohn* – rendu en 1975[311], portait sur la constitutionnalité d'une disposition de l'*Official Code of Georgia Annotated*[312] qui incriminait la divulgation par quelque moyen que ce soit du nom de la victime d'un viol ou d'une tentative de viol, ainsi que celle du *tort of public disclosure* prévu par une loi de l'État. En 1971, une adolescente de 17 ans avait été violée par six jeunes gens. Elle fut retrouvée morte. Le procès des co-accusés s'ouvrit huit mois plus tard et un journaliste, qui couvrait l'événement pour la télévision qui l'employait, prit connaissance du nom de la victime en consultant *légalement* l'acte d'accusation. Dès le lendemain, la télévision diffusait le nom de la victime. Le père de la victime introduisit alors une action contre le propriétaire du journal, arguant de la violation de la loi incriminant la divulgation du nom des victimes de viol et d'une atteinte portée à la vie privée par divulgation de l'identité de sa fille. La Cour Suprême a d'abord reconnu que « [d]ans ce domaine de conflit entre revendications de vie privée et revendications de liberté de la presse, les intérêts ont, de part et d'autre, leurs racines dans nos traditions, et représentent des préoccupations majeures de notre société ». Pleine de prudence, elle a également rappelé que « [p]lutôt que d'aborder la question plus large de savoir si des publications sincères <*truthful publications*> peuvent jamais être soumises à une responsabilité civile ou pénale et ce en conformité avec les Premier et Quatorzième amendements [...], il convient de mettre l'accent sur l'interface étroite entre presse et vie privée que cette affaire présente ». En d'autres termes, il convenait de déterminer si « l'État peut imposer des sanctions pour la publication exacte du nom de la victime d'un viol obtenu à partir des dossiers publics – et plus précisément des dossiers judiciaires qui sont en lien avec l'exercice des poursuites et qui sont ouverts à l'examen du public ». La Cour a conclu que l'État ne pouvait pas.

Après *Cox*, la Cour suprême a apporté deux séries de précisions. L'arrêt *Oklahoma Publishing Co. v. Oklahoma County District Court*, de 1977[313], a tout d'abord permis à la Haute juridiction de préciser que, en interdisant à des journalistes, qui avaient pu assister au procès pénal d'un mineur de 11 ans, de publier son nom et sa photographie, l'État violait le Premier amendement[314]. À l'occasion

---

309 V., en particulier, E. Volokh, « Freedom of Speech and Information Privacy : The Troubling Implications of a Right to Stop People from Speaking About you », op. cit., spéc. p. 1091-1092 ; T.M. Funk, « The Danger of Hiding Criminal Pasts », 66 Tenn. L. Rev. 287 (1998).

310 Wilan v. Columbia County, (280 F.3d 1160, 1163 (7th Cir. 2002).

311 Cox Broadcasting Corp v. Cohn, 420 U.S. 469 (1975).

312 Ga. Code Ann. § 26-9901 (1972).

313 Oklahoma Publishing Co. v. Oklahoma County District Court, 430 U.S. 308 (1977).

314 En l'occurrence, la loi de l'État de l'Oklahoma ordonnait le huis clos pour toutes les procédures contre les mineurs, à moins que le juge ait expressément autorisé la publicité des débats. Le texte limitait également l'accès aux dossiers judiciaires aux personnes justifiant d'un intérêt légitime et y ayant été expressément autorisées par la Cour

de l'affaire *Smith v. Daily Mail Publishing Co.*, de 1979[315], était en débat la constitutionnalité d'un délit punissant la publication du nom d'un accusé mineur, sans autorisation de la cour[316]. En l'occurrence, deux journaux avaient publié le nom et la photographie d'un garçon de 15 ans poursuivi pour avoir tué par arme à feu l'un de ses camarades de classe âgé de 14 ans. Par une opinion particulièrement bien motivée, la Cour devait retenir que l'État ne pouvait pas, sans méconnaître les Premier et Quatorzième amendements, punir un journal pour avoir publié le nom, *légalement obtenu*, d'un accusé mineur. La protection de l'anonymat du mineur, garantie de sa réinsertion, n'a pas été jugée suffisante pour justifier l'imposition de sanctions criminelles.

47. Mais c'est le célèbre arrêt The Florida Star *v. B.J.V.*, rendu en 1989[317], qui a porté le coup fatal à la jurisprudence *Briscoe*. Était en jeu, en l'occurrence, l'une de ces lois dont il a déjà été fait état interdisant la publication, quelle qu'en soit la forme, du nom d'une victime d'une agression sexuelle. En 1983, B.J.F, la victime dont seules les initiales ont été conservées, dénonçait à la police un vol et une agression sexuelle dont elle disait avoir été victime. À la suite d'une négligence de la police, son nom complet était introduit dans le rapport de police destiné à la salle de presse. Un journaliste stagiaire en prit connaissance et copie, et un reporter du *Florida Star* publia un article divulguant l'identité de la victime, en violation des règles de déontologies du journal. Près d'un an plus tard, la victime introduisait une action contre le département de police et contre le journal, alléguant que les défendeurs avaient, par négligence, violé le texte évoqué ci-dessus. Pour les premiers juges, la disposition litigieuse était constitutionnel, car établissant un équilibre adéquat entre la protection de la liberté d'expression et la vie privée. Ils accordèrent, en conséquence, $75 000 de dommages intérêts compensatoires et $25 000 de dommages intérêts punitifs. Dans son arrêt d'annulation, la Cour Suprême refuse de suivre la jurisprudence *Cox* et décline surtout l'invitation des requérants à statuer largement en faveur de la liberté d'expression et de la presse ; c'est que, dit-elle, « [n]os arrêts ont soigneusement évité d'atteindre cette ultime question, pleinement conscients de ce que l'avenir nous réserve sans doute de nouveaux scénarios que la prudence nous conseille de ne pas résoudre par anticipation ». La portée de l'arrêt n'en est pas moins grande qui vient s'enter sur le motif décisoire de l'arrêt *Daily Mail* : « si un journal obtient légalement des informations sur une question importante pour le public, alors les agents de l'État ne peuvent, sans violer la Constitution, punir la publication de l'information, en l'absence d'une nécessité [...] de premier ordre *<need...of the highest order>* »[318]. Les intérêts avancés par l'État sont évidemment légitimes. Qu'il s'agisse de protéger la vie privée ou l'intégrité physique des victimes d'infractions sexuelles, qu'il s'agisse de les encourager à témoigner en les

---

(cf. Okl.Stat.Ann., Tit. 10, §§ 1111, 1125 (Supp.1976)).- Il n'est pas nettement établi si, en l'espèce, les journalistes avaient été expressément autorisés à assister à la procédure. Pour la Cour, les informations n'en ont pas moins été légalement obtenues.

315 Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).

316 W. Va. Code 49-7-3 (1976) : « [N]or shall the name of any child, in connection with any proceedings under this chapter, be published in any newspaper without a written order of the court [...] » ; « A person who violates [...] a provision of this chapter for which punishment has not been specifically provided, shall be guilty of a misdemeanor, and upon conviction shall be fined not less than ten nor more than one hundred dollars, or confined in jail not less than five days nor more than six months, or both such fine and imprisonment ».

317 The Florida Star v. B.J.V. 491 U.S. 524 (1989).

318 Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979), spéc. p. 103.

préservant d'une exposition médiatique, voilà autant de raisons qui pourraient conduire l'État à encadrer la liberté d'expression. Mais il existe à l'évidence des moyens moins drastiques – tel le recours à l'anonymat – pour préserver ces intérêts importants.

Sans doute est-il possible d'interpréter l'affaire *Florida Star* étroitement, comme laissant intacte la possibilité pour l'État d'encadrer étroitement la divulgation et la republication de certaines informations, en certains contextes[319]. La passe est, en tout cas, étroite, et comme l'ont remarqué de nombreux auteurs, si le *tort of public disclosure* est « vivant, il est sous assistance respiratoire »[320]. Et il y a donc peu de chance que ce *tort* puisse jamais assurer, comme autrefois dans les affaires *Melvin* (« Le Kimono Rouge ») et *Briscoe*[321], une forme de droit à l'oubli, sauf à pouvoir se renforcer, comme cela arrive parfois, de l'omnipotent Premier amendement.

B- Éloge du libre discours : le retour à la vie privée ?

48. L'insatisfaction provoquée par cette jurisprudence restrictive a manifestement stimulé l'inventivité de la doctrine qui a souligné le potentiel de plusieurs décisions rendues autour du Premier amendement. La première qui mérite attention – *Cohen v. Cowles Media Co.*[322] – concernait un accord de confidentialité conclu entre un journaliste et sa source dont le nom devait rester secret. Son identité fut néanmoins publiée par le journaliste, en méconnaissance de son engagement. L'informateur du journaliste poursuivit le journaliste et obtint des dommages intérêts sur le fondement du *promissory estoppel*. Le journaliste se retrancha dernière le Premier amendement et la jurisprudence *Florida Star* ; mais en vain. Selon la Cour Suprême, en effet, « les lois d'application générale ne heurtent pas le Premier amendement simplement parce que leur mise en œuvre contre la presse a un effet secondaire sur son aptitude à réunir et relater des actualités ». Au-delà de la mise en échec du Premier amendement – l'État ne limitant plus

---

319 V., en ce sens, D.J. Solove, « The Virtues of Knowing Less : Justifying Privacy Protections Against Disclosure », op. cit., spéc. p. 1022-1023 : « Nevertheless, this case can be read very narrowly. The Court suggested that the Florida statute was far too broad. The statute applied "regardless of whether the identity of the victim is already known throughout the community; whether the victim has voluntarily called public attention to the offense; or whether the identity of the victim [had] otherwise become a reasonable subject of public concern." The law focused only on the nature of the information, rather than on whether each particular use of a rape victim's name in a specific context would be of public or private concern. Florida Star can be construed to suggest that a law adopting a less categorical approach – by addressing the use of the identifying data more contextually – might not be subject to strict scrutiny under the First Amendment ».- V. toutefois les remarques de F. Werro, « The Right to Inform v. the Right to be Forgotten : A Translatlantic Clash », in A. Colombi Ciacchi et al. (ed.), Haftungsrecht im dritten Millenium.- Liber Amicorum Gert Brüggemeier, Nomos, Baden Baden, 2009, p. 285 et s., spéc. p. 296-297.

320 R.S. Murphy, « Property Rights in Personal Information : An Economic Defense of Privacy », 84 Geo L.J. 2381 (1996), spéc. p. 2388. V. aussi R. Smolla, « Privacy and the First Amendment Right to Gather News », Geo. Wash. L. Rev. 1097 (1999) ; Ph.E. DeLaTorre, « Resurrecting a Sunken Ship : An Analysis of Current Judicial Attitudes Toward Public Disclosure Claims », 38 Sw. L.J. 1151 (1985), spéc. p. 1184 ; J.K. Rolfs, « The Florida Star v. B.J.F. : The Beginning of the End for the Tort of Public Disclosure », Wis. L. Rev. 1107 (1990), spéc. p. 1128 ; F. Werro, art. préc., p. 296 ; R.K. Walker, « The Right to Be Forgotten », 64 Hastings L.J. 257 (2012), spéc. p. 268.

321 La Cour Suprême de Californie a d'ailleurs abandonné son précédent en 2004 (Gates v. Discovery Communications, Inc., 101 P.3d 552, (Cal. 2004), spéc. p. 559, 561-562), jugeant, en particulier, que la jurisprudence de la Cour Suprême des États-Unis en matière de divulgation ne se prêtait à aucune distinction au regard de la nature, récente ou ancienne, des faits rapportés par la presse.

322 Cohen v. Cowles Media Co., 501 U.S. 663 (1991).

l'expression, mais apportant son concours à l'exécution d'une obligation[323] –, la force de cet arrêt est sans doute de permettre la reconnaissance d'engagements (« *promises* ») de confidentialité implicites (« *implied contracts or terms of confidentiality* »)[324] ou tirés de la doctrine du *promissory estoppel*[325], et ce à partir[326] d'une *espérance de vie privée*[327]. L'autre intérêt de ces engagements est de

---

323 R.K. Walker, « The Right to be Forgotten », op. cit., p. 277-279 ; V. Samuelson, « Privacy as Intellectual Property ? », 52 Stan. L. Rev. 1125 (2000), p. 1155-1557. Cf., plus généralement, S. Shorr, « Personal Information Contracts : How to Protect Privacy Without Violating the First Amendment », 80 Cornell L. Rev. 1756 (1995).

324 Selon le Restatement (Second) of Contracts, § 4 (« How a Promise May Be Made » – trad. « De la forme de l'engagement »), « [u]n engagement peut être formulé avec des mots, qu'ils soient écrits ou exprimés oralement, ou être inféré, en tout ou partie, de la conduite ». Dans le commentaire a) qui l'assortit, il est précisé qu'une distinction est ainsi faite entre contrats exprès et implicites. Certains termes du contrat sont souvent implicites (« implicit terms »). Ils trouvent parfois leur origine dans un précédent ou la loi (par ex., sous l'empire du Uniform Commercial Code, § 2-306(2), lorsque vendeur et acheteur sont liés par un contrat d'exclusivité, une obligation implicite de diligence (« best efforts ») s'ajoute au contrat) ; on parle alors de clauses « implied-in-law ». Certaines obligations se dégagent des circonstances qui entourent la formation d'un contrat, comme les précédentes transactions entre les parties, les usages de l'industrie, la définition spécifique d'autres dispositions contractuelles, etc. On parle alors de clauses « implied-in-fact ». V. aussi : R.K. Walker, « The Right to Be Forgotten », op. cit., spéc. p. 278.

325 Une des conditions de validité du contrat dans les droits de Common Law est l'existence d'une consideration ; une promesse n'engage en principe son auteur sur le terrain contractuel que si son bénéficiaire a fourni une contrepartie – ou plusieurs contreparties – au promettant. En certaines hypothèses, cette exigence a paru si contraignante que les juridictions d'Equity ont développé une nouvelle doctrine, celle de l'estoppel. Cette doctrine n'est pas uniforme et une étude récente a pu dénombrer plus d'une douzaine de formes d'estoppel (E. Cooke, The Modern Law of Estoppel, OUP, Oxford, 2000). Il n'est guère que dans l'un de ces effets possibles que toutes les formes d'estoppel conjoignent. Le plaideur a « bâillon aux lèves » et il se trouve ainsi dans l'impossibilité de soutenir un fait contraire à celui a été constaté par les juges. L'image correspond d'ailleurs bien à la signification du mot du vieux français – estoupper – dont l'estoppel tire son origine : « [...] de même qu'on utilise un tampon d'étoupe pour obstruer une voie d'eau qui, malencontreusement s'est produite dans une paroi, ainsi un plaideur emploie-t-il le moyen de l'Estoppel au cours d'un procès judiciaire, comme il mettrait un bâillon aux lèvres de son adversaire, pour lui interdire péremptoirement d'alléguer telle prétention qui serait en contradiction flagrante avec certains faits auxquels s'attache un caractère de vérité incontrovertible : et ceci a pour résultat de simplifier singulièrement les procédures » (J. Dargent, La doctrine de l'estoppel.- Une théorie originale du droit anglais en matière de preuve, Imprimerie Georges Frère, Tourcoing, 1943, p. 3). On doit le développement du promissory estoppel à un célèbre obiter dictum de Lord Denning J, dans l'affaire Central London Property Ltd v High Trees House Ltd ([1947] KB 130), qui en a donné la définition : « lorsque, par mots ou conduite, une personne fait une representation univoque quant à sa conduite future, avec l'intention <intending the representation to be relied on> de faire de la representation un fondement à l'action et d'affecter les relations juridiques entre les parties, tandis que le Recipiens modifie sa position sur la foi de celle-ci, l'Agens [l'auteur de la representation] se verrait privé de la possibilité d'agir en contradiction avec cette representation si, ce faisant, le Recipiens [le destinataire de la representation] en subissait un préjudice ». Il est impossible de développer plus avant, mais il faut au moins indiquer les principales conditions de la doctrine : au-delà de l'existence d'une relation contractuelle entre les parties, il est nécessaire qu'il y ait une promesse ou une representation portant sur une conduite future, animée par l'intention d'affecter les relations juridiques entre les parties ; la promesse doit avoir servi de support à la position du Recipiens (« the promissee must have acted in reliance on the promise ») ; en d'autres termes, la representation doit avoir influencé la conduite du Recipiens. Certains dicta laissent entendre qu'il faudrait que le Recipiens montre sa « detrimental reliance », c'est-à-dire qu'il subirait un préjudice si l'Agens était autorisé à exercer son droit pour lequel il est estopped ; en tant que doctrine d'Equity, enfin, le promissory estoppel suppose la démonstration qu'il serait « inéquitable/injuste » (inequitable) d'autoriser l'Agens à revenir sur sa promesse ou sa representation. Le promissory estoppel est également connu du droit américain, dont le Restatement (Second) of Contracts, § 90 (à la différence du premier Restatement) donne une définition plus large en reconnaissant également la detrimental reliance du tiers à la promesse (v. infra, n° 53). Les tribunaux américains se prononcent plus souvent sur le fondement la « théorie de la confiance » (« reliance

laisser hors du débat la question de l'*impact* de la divulgation des faits sur une personne raisonnable. Les « engagements de vie privée » articulent l'examen du juge autour du résultat recherché par l'émetteur : « le destinataire de l'information personnelle ne peut utiliser l'information que pour les finalités auxquelles [l'émetteur] a consenti, et rien d'autre »[328]. On mesurera mieux les potentialités de cette doctrine en étudiant la vie privée informationnelle et le droit à l'oubli[329].

49. Par une autre décision importante, la Cour Suprême est également venue suggérer que, en certaines circonstances, la vie privée pouvait se réclamer de la protection du Premier amendement, contribuant possiblement à redéfinir les équilibres entre liberté d'expression (liberté de la presse) et vie privée[330]. Il s'agit de l'arrêt *Bartnicki v. Vopper*, rendu en 2001 par la Cour Suprême[331]. Il faut, comme toujours, s'attacher aux faits de l'espèce qui expliquent, le cas échéant, les analogies et distinctions faites par la Cour. Des négociations décrites comme tendues avaient débuté entre un syndicat (« *Union* ») enseignant (*Pennsylvania State Education Association*) de l'École *Wyoming Walley West High* et le conseil scolaire. En 1993, la demanderesse Bartnicki, négociatrice principale pour le compte du syndicat, utilisait le téléphone cellulaire de son véhicule pour appeler

---

theory » ou « promissory reliance ») qui est cependant tout à fait comparable : (1) le promettant savait ou aurait dû savoir que le bénéficiaire de la promesse était susceptible de se fonder sur la promesse ; (2) le bénéficiaire de la promesse s'est effectivement fondé sur la promesse ; (3) la confiance du bénéficiaire était raisonnable ; (4) le bénéficiaire a subi un préjudice consécutif à cette confiance ; (5) l'injustice ne peut être évitée qu'en donnant exécution à la promesse (cf. I.S. Russell, B.K. Bucholtz, Mastering Contract Law, Carolina Academic Press, Durham, 2011, p. 187).

326 R.K. Walker, op. cit., loc. cit.

327 E. Volokh, « Freedom of Speech and Information Privacy : The Troubling Implications of a Right to Stop People from Speaking About You », 52 Stan. L. Rev. 1049 (2000), spéc. p. 1058-1059 : « Dans de nombreux contextes, les gens espèrent raisonnablement – en raison des usages, de l'habitude de traiter avec l'autre partie, ou tout autre facteur pertinent pour identifier un contrat implicite – qu'une partie de ce à quoi s'est engagé son cocontractant est la confidentialité ».- Toutefois, comme l'a remarqué Paul Schwartz, la proposition de Volokh est ambiguë, parce qu'elle paraît reposer sur l'existence de dispositions supplétives de volonté (« default statutes », « non-mandatory rules ») identifiant certaines transactions dont il est ensuite présumé qu'elles contiennent des engagements de confidentialité (P.M. Schwartz, « Free Speech vs. Information Privacy : Eugene Volokh's First Amendment Jurisprudence », 52 Stan. L. Rev. 1559 (2000), spéc. p. 1570). Les grandes limites de ces solutions contractuelles résident dans l'effet relatif du contrat (« privity of contract » – E. Volokh, op. cit., p. 1061) et dans la possibilité reconnue aux parties d'aménager des règles contraires (P.M Schwartz, op. cit., p. 1569 et s.).

328 V. Mayer-Schönberger, Delete..., op. cit., p. 136.- V. aussi N.M. Richards, D.J. Solove, « Privacy's Other Path : Recovering the Law of Confidentiality », 96 Geo. L.J. 123 (2007), spéc. p. 130-132.

329 V. infra, n° 53.

330 Il a pareillement pu être observé que le Premier amendement avait moins de poids lorsqu'étaient en jeu des communications internationales. V., par ex., Yahoo !, Inc. v. La Ligue Contre le Racisme et l'Antisémitisme (433 F.3d 1199 (9th Cir. 2006), renversant une décision qui refusait, pour des motifs tirés du Premier amendement, de donner force exécutoire à une ordonnance de référé rendue par le TGI de Paris (22 mai 2000 – Légipresse 2000, n° 147, p. 139-146, obs. C. Rosinsky) enjoignant à Yahoo de faire cesser la vente d'objets nazis sur son site. La juridiction américaine notait, en particulier : « l'étendue de la protection offerte par le Premier amendement à un discours accessible seulement en dehors des États-Unis est difficile et, dans une certaine mesure, non réglée ». Plus récemment, dans Holder v. Humanitarian Law Projet (130 S. Ct. 2705 (2010)), la Cour Suprême a confirmé des dispositions du USA Patriot Act qui criminalisent la libre expression lorsqu'elle est en lien avec des organisations terroristes étrangères.

331 Bartnicki v. Vopper 532 U.S. 514 (2001).

Kane, également demandeur, alors président du syndicat. À l'occasion de cette conversation, qui fut enregistrée à leur insu, Kane tint les propos suivants : « "S'ils ne bougent pour 3%, on va devoir aller chez, chez eux... Pour faire sauter leurs porches, on va devoir faire un truc à certains de ces gars. (PAUSE) Vraiment, euh, vraiment, je t'assure, parce que ça, tu vois, ça c'est une mauvaise nouvelle" (INCOMPRÉHENSIBLE) ». Il n'est pas contesté que l'information fut ensuite transmise, par l'auteur anonyme de l'interception, à Jack Yocum, chef d'une organisation de contribuables locaux qui s'était opposée aux demandes du syndicat au cours des négociations. C'est ce dernier qui remit l'enregistrement au défendeur Vopper, animateur d'une émission politique radiodiffusée, qui le porta pour la première fois à la connaissance du public. Arguant de la violation de dispositions fédérale et étatique réprimant la divulgation du contenu de conversations illégalement interceptées[332], les demandeurs réclamaient des dommages intérêts compensatoires (*actual damages*), légaux (prévus par un texte de loi – *statutory damages*) et punitifs (*punitive damages*). En premier lieu, la Cour reconnaît que la question du degré de protection que le Premier amendement accorde, le cas échéant, au discours divulguant le contenu d'une communication illégalement interceptée est « inédite et étroite ». Elle souligne également trois données factuelles importantes : 1° Les défendeurs n'ont joué aucun rôle dans l'interception. Ils ont au contraire trouvé l'enregistrement après coup et ignorent toujours qui a pratiqué cette interception ; 2° Il a été accédé légalement à l'information contenue dans ses enregistrements, bien que l'interception ait été pratiquée de manière illégale ; 3° Le sujet de la conversation était une question d'intérêt public. Et si les déclarations, dit la Cour, avait été faite dans une arène publique – durant la session de négociation, par exemple –, elles auraient été dignes de faire l'actualité (*newsworthy*). La chose aurait été identique si une tierce-personne avait, de manière fortuite, entendu les propos de Bartnicki.

50. De toute manière, juge la Cour, rappelant son précédent *Smith v. Daily Mail Publishing Co.*[333], « l'action de l'État destinée à punir la publication d'informations exactes <*truthful information*> ne peut presque jamais satisfaire les standards constitutionnels ». Et la formule désormais classique, reprise dans l'arrêt *Florida Star*, revient naturellement sous la plume : « si un journal obtient légalement des informations sur une question importante pour le public, alors les agents de l'État ne peuvent, sans violer la Constitution, punir la publication de l'information, en l'absence d'une nécessité… de premier ordre <*need…of the highest order*> ». Si l'État pouvait se prévaloir d'intérêts légitimes – tel dissuader les interceptions illégales ou limiter le préjudice de ceux dont les conversations ont été interceptées –, ils n'étaient pas suffisamment importants pour tenir en échec le Premier amendement. Comme l'énonce la Cour :

> « En l'espèce, les intérêts attachés à la vie privée cèdent le pas lorsqu'ils sont mises en balance avec l'intérêt que représente la publication de question d'importance

---

332 L'infraction fédérale suivante était concernée : 18 U.S.C. § 2511(1)(c) : une personne qui « intentionnellement, divulgue ou tente de divulguer à autrui, le contenu d'une communication orale, téléphonique ou électronique, tout en sachant ou en ayant des raisons de croire que l'information a été obtenue au moyen de l'interception d'une communication orale, téléphonique ou électronique en violation de cette sous-section, … sera punie… ». La disposition équivalente de l'État de Pennsylvanie était également en jeu : 18 Pa. Cons. Stat. §5725(a) (2000).

333 Smith v. Daily Mail Publishing Co., 443 U.S. 97, 102 (1979).

publique » ; « [l]'un des coûts associés à la participation aux affaires publiques est la perte correspondante de vie privée ».

Sur chacun de ces points, des objections sérieuses ont été élevées par les juges dissidents. La doctrine a également dénoncé l'attitude paradoxale de la Cour consistant à reconnaître le caractère neutre (*content-neutral*) des textes en jeu, tout en les soumettant à un contrôle étroit. Mais c'est sur un autre point que l'arrêt interroge, montrant tout à la fois les limites de sa propre cohérence et les ressources de son propre dépassement.

51. Comme le notait déjà le juge Breyer dans son opinion concordante, à laquelle est venu se joindre le juge O'Connor, « [c]e que la Cour a appelé "contrôle strict" <*strict scrutiny*> – avec sa forte présomption de non-constitutionnalité – ne convient normalement pas lorsque, comme en l'espèce, d'importants intérêts constitutionnels concurrents sont impliqués. Les restrictions légales <*statutory restrictions*> devant nous promeuvent directement le discours privé. Les dispositions légales garantissent la confidentialité <*privacy*> des conversations téléphoniques. [...] Cette garantie de vie privée nous aide à surmonter notre réticence à discuter d'affaires privées, réticence attachée à la crainte que nos conversations privées puissent devenir publiques ». C'est sur ce paradoxe qu'a également beaucoup insisté le juge Rehnquist dans une opinion dissidente de poids à laquelle sont venus se joindre les juges Scalia et Thomas. Ce que notent, là encore, les juges, c'est que le raisonnement de la Cour aboutit paradoxalement, en se réclamant du Premier Amendement, à une solution qui amoindrit la liberté d'expression des millions d'Américains qui utilisent quotidiennement les technologies électroniques pour communiquer. Comme le note encore le juge, ces « lois protègent indéniablement ce vénérable droit à la vie privée » ; et, « dans le même temps, elles font avancer les droits des parties à la conversation ». S'appuyant sur les précédents *Turner Broadcasting System, Inc. v. FCC* et *New York Times Co. v. Sullivan*, les juges dissidents soulignent fort pertinemment que « [s]e trouve au cœur du Premier amendement le principe selon lequel chaque personne devrait pouvoir décider pour elle-même les idées qui méritent d'être exprimées, prises en considération et respectées »[334] et qu'« en protégeant la confidentialité <*privacy*> de la pensée et de l'expression de chacun », ces lois promeuvent « l'expression forte, libre et ouverte »[335] des citoyens. On rejoint aussi bien les potentialités du Premier amendement, parfaitement dévoilées par l'arrêt *Hurley*, sur lequel s'appuie également l'opinion dissidente : « l'une des dimensions importantes du principe du libre discours est que celui qui choisit de parler peut aussi décider "ce qu'il ne veut pas dire" »[336]. L'expression, le discours, n'est pas simplement un contenu, mais une interaction, c'est-à-dire un rapport entre un *individu* et une *audience*[337]. Le Premier amendement permet d'aménager des zones protégées à l'intérieur desquelles peut être exprimé ce que nous ne voulons pas dire – *ne pas dire à une plus large audience*[338]. Ainsi devraient se penser, dans une version renouvelée, les rapports entre vie privée et

---

334 Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622 (1994).

335 New York Times Co. v. Sulllivan, 376 U.S. 254 (1964).

336 Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston, Inc., 515 U.S. 557 (1995).

337 P. Gewirtz, « Privacy and Speech », 2001 Sup. Ct. Rev. 139 (2001), spéc. p. 154-155.

338 Cf. Wooley v. Maynard, 430 U.S. 705 (1977), p. 714 : « Le droit de parler et le droit de s'abstenir de parler sont des éléments complémentaires du concept plus large de "liberté d'esprit du chacun" » ; Pac. Gas. & Elec. Co. v. Pub. Utils. Comm'n, 475 U.S. 1 (1986), p. 11 : « le Premier amendement contient la "liberté de ne pas parler

liberté d'expression ; une vie privée qui, derrière l'enceinte du Premier amendement, deviendrait *liberté de dire* ou *de ne pas dire*, maîtrise dans la sphère informationnelle comme condition essentielle de la liberté d'expression et, plus loin, participation à la sphère publique (*vita activa*). En se détachant de toute référence au contenu, la *privacy* se sépare du droit « d'absolue immunité »[339]. Elle se métamorphose en liberté et se rapproche insensiblement de la philosophie qui gouverne la protection des données.

Section 3 - Le droit à l'oubli et la protection des données

52. L'extrême complexité qu'on a pu constater dans le domaine de la protection de la vie privée se constate également dans celui de la protection des données. Il ne faut pas s'attendre à trouver un texte qui serait l'équivalent de la loi française « Informatique et Libertés » et une autorité administrative qui, à l'instar la Commission Nationale de l'Informatique et des Libertés, serait chargée d'autoriser et de réguler les traitements de données. Conformément à l'esprit pragmatique qui l'anime, le droit américain s'est surtout attacher à répondre, chaque fois qu'ils se présentaient, à des problèmes particuliers, sans véritable vision d'ensemble. D'où ce constat, dans le domaine qui nous occupe, d'une protection sectorielle et défaillante (I). Il n'en faut pas moins souligner le rôle complémentaire et grandissant qu'occupe aujourd'hui la *Federal Trade Commission* (II).

I- Une protection sectorielle et défaillante

53. Si le législateur (fédéral, étatique) a éprouvé le besoin d'intervenir, c'est bien parce que les solutions disponibles n'étaient pas adaptées. Les *privacy torts*, ponctuellement utilisés, ont montré leurs faiblesses. Dans l'affaire *Dwyer v. American Express Co.*[340], des porteurs de cartes bancaires émises par American Express se plaignaient de ce que l'établissement financier américain vendait des données sur leurs comportements d'achat. La juridiction devait rejeter l'action fondée sur le *tort* d'intrusion, matérielle ou non, dans l'intimité ou la solitude de l'individu[341] (« *intrusion upon seclusion tort*), motif pris de ce que la première condition du *tort*, à savoir l'intrusion non autorisée n'était pas satisfaite. À l'inverse, les informations avaient été transmises volontairement : « En utilisant sa carte American Express, le porteur de carte donne volontairement et nécessairement aux défendeurs des informations qui, une fois analysées, révèlent les habitudes d'achat et les préférences commerciales des porteurs de cartes [...] ». Dans une affaire plus ancienne[342], c'était le *tort of public disclosure* qui était écarté dans le cadre d'une

---

publiquement", liberté qui sert la même fin ultime que la liberté d'expression dans sa dimension positive » ; W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624 (1943), p. 645 ; arrêts cités par R.K. Walker, « The Right to be Forgotten », op. cit., p. 277.- Adde, R.A. Sedler, « The First Amendment Right to Silence », Wayne State University Law School Research Paper No. 07-39, November 9, 2007 ; M. Scott, « The Hidden First Amendment Values of Privacy », 71 Wash. L. Rev. 683 (1996), spéc. p. 717.

339 Selon la célèbre formule de Cooley citée dans Union Pacific Ry. C. v. Botsford, 141 U.S. 250, 251 (1891) ; v. supra, note (109).

340 Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. 1995).

341 V. supra, n° 14.

342 In Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975).

action dirigée contre plusieurs magazines qui avaient vendu leurs listes d'abonnés à des entreprises de prospection commerciale par voie postale. C'est que, pour la juridiction, il n'était pas établi en quoi la divulgation de ces listes (révélant assurément le mode de vie des abonnés) était propre à infliger, à une personne de sensibilité ordinaire, une souffrance morale ou provoquer sa honte ou son humiliation. Déplaçant la réflexion sur le terrain du droit des contrats, une partie de la doctrine a proposé d'interpréter les politiques de confidentialité comme des contrats, bien que les termes en soient fixés unilatéralement par l'entreprise et ne soient pas négociables[343]. Les affaires portées devant les juridictions fédérales n'ont pas connu plus de succès que celles fondées sur les *torts*. Les juridictions n'ont d'ailleurs pas manqué d'arguments pour écarter les demandes : une absence de contrat (*unilateral contract*), au motif que les « déclarations de politique générale ne sont pas contractuelles », et les politiques de confidentialité ne sont rien d'autre, car le langage utilisé laisse généralement toute discrétion à l'opérateur du site en ce qui concerne la détermination de la pertinence de l'information et de la « tierce-partie qui pourrait avoir besoin de cette information »[344] ; une absence d'acceptation, n'étant pas démontré que les demandeurs ont effectivement lu la politique de confidentialité[345] ; une absence de dommage[346], pour le moins de dommage réparable, ce que n'est pas la « perte de vie privée »[347].

---

343 On doit cette analyse à cet auteur, en particulier : S. Killingsworth, « Minding Your Own Business : Privacy Policies in Principles and in Practice », 7 J. Intell. Prop. L. 57, (1999).

344 In re Northwest Airlines Privacy Litigation 2004 WL 1278459 (D. Minn. 2004) (non publié dans le F. Supp. 2d). Dans cette affaire, dont le cadre constitue la politique de renforcement de la sécurité aérienne après le 11 septembre, la compagnie Northwest Airlines, Inc. avait transmis à la NASA, sur sa demande, les données de dossiers passagers (« passengers name records » ou « PNRs ») qui sont des dossiers électroniques contenant des informations telles que le nom du passager, son numéro de vol, des données relatives à sa carte de crédit, sa réservation d'hôtel, sa location de véhicule et ses compagnons de voyage. Pour les demandeurs, passagers de la compagnie aérienne, cette pratique constituait une violation de l'Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 et s., du Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, ainsi que du Minnesota's Deceptive Trade Practices Act (DTPA), Minn. Stat. § 325D. Les plaignants invoquaient également une atteinte à la vie privée, une atteinte à la propriété (« trespass in property »), une negligent misrepresentation et, surtout, une violation du contrat les liant à la compagnie aérienne et qu'ils identifiaient, en l'occurrence, dans la politique de confidentialité du site Internet de l'entreprise, énonçant, en particulier, que la compagnie aérienne ne partagerait pas les informations personnelles des passagers, hormis pour organiser leur voyage.

345 In re Northwest Airlines Privacy Litigation (et le fait qu'ils se soient « appuyés » sur cette politique n'est pas suffisant) ; la conclusion est identique dans cette autre affaire qui mettait également en jeu la divulgation par Northwest Airlines de dossiers passagers au gouvernement : Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004).

346 Dyer v. Northwest Airlines Corp., op. cit.. Ainsi que l'indique la juridiction, même si la politique de confidentialité avait été suffisamment définie et même si les plaignants avaient établi qu'ils avaient effectivement lu la politique avant de fournir leurs informations, les plaignants n'ont établi aucun dommage résultant de la prétendue violation du contrat.

347 Trkias v. Universal Card Services Corp., 351 F. Supp. 2d 37 (E.D.N.Y.). La Cour rappelle le principe : « la réparation en droit des contrats, à la différence de la réparation en droit de la responsabilité civile, est ouverte seulement pour les pertes économiques découlant directement de la violation ». C'est que, en droit des contrats, la responsabilité est seulement destinée à replacer l'individu dans la position économique qui aurait été la sienne si le contrat avait été pleinement exécuté.

L'avenir nous dira, enfin, si les propositions qui sont actuellement faites en faveur d'une application du mécanisme du *promissory estoppel* sont traitées avec une plus grande faveur[348].

54. En l'état actuel du droit américain, c'est la loi qui offre le cadre le plus développé de protection des données personnelles et le fondement immédiat d'un possible droit à l'oubli. Disons-le d'emblée, le cadre est loin d'être satisfaisant : non seulement parce qu'il est formé d'un labyrinthe de texte inadaptés (A) ; mais plus encore parce que la jurisprudence tend à assimiler le traitement de données à un discours commercial protégé par le Premier amendement (B).

A- Un labyrinthe de textes inadaptés

55. Dans le domaine commercial – seul évoqué dans les lignes qui suivent – plusieurs textes sont potentiellement applicables à la collecte, l'utilisation et au transfert de données personnelles. L'approche du Congrès (et la remarque est la même pour les législateurs des États) a été sectorielle, c'est-à-dire circonscrites à certaines catégories d'activités commerciales et de services. À la différence de la plupart des États européens, les États-Unis ne disposent donc d'aucun texte général[349]. Trois grands domaines seulement ont été réglementés : celui du divertissement, avec la vidéo[350] et la télévision par câble[351] ; celui de l'Internet et des communications électroniques[352] ; celui, enfin, du marketing, avec une attention toute particulière portée aux activités de télémarketing[353] et de spamming[354]. Deux textes, en particulier, méritent d'être interrogés sous l'angle du droit à l'oubli : le *Electronic Communications Privacy Act* (EPCA) et le *Children's Online Privacy Protection Act* (COPPA).

---

348 Sur le promissory estoppel, v. supra, n° 48— Le fondement serait le Restatement (Second of Contracts), § 90 : « Une promesse dont le promettant peut raisonnablement s'attendre à ce qu'elle incite à une action ou à une abstention du bénéficiaire de la promesse ou d'une tierce-personne et qui incite effectivement à une telle action ou abstention, est obligatoire si l'injustice ne peut être évitée qu'en donnant exécution à la promesse. Le remède accordé pour violation peut être limité à ce que la justice commande » (cf. I.S. Russell, B.K. Bucholtz, Mastering Contract Law, op. cit., spéc. p. 188-190). Selon un auteur (W. Hartzog, « Promises and Privacy : Promissory Estoppel and Confidential Disclosure in Online Communities », 82 Temp. L. Rev. 891 (2009), spéc. p. 893-896.), on pourrait admettre le jeu du promissory estoppel entre les membres d'un réseau social, chacun étant en droit de s'attendre à la confidentialité des données qu'il a choisi de divulguer à quelques personnes seulement. Le même auteur (W. Hartzog, « Website Design as Contract », 60 Am. U. L. Rev. 1635 (2011)) a proposé d'utiliser la doctrine du promissory estoppel pour remédier aux conséquences dommageables des changements inopinés de politiques de confidentialité sur les réseaux sociaux. Pour établir la representation, il suffirait de donner foi, non aux politiques de confidentialité ou aux accords d'utilisation du site – qui ne sont généralement pas lus par les utilisateurs –, mais aux paramètres de confidentialité (« privacy settings »), ainsi qu'à tout autre élément du site qui permet à l'utilisateur de préciser ses préférences en matière de vie privée.

349 D. Solove, P. Schwartz, Information Privacy, op. cit., p. 839 et s.

350 Video Privacy Act (VPPA) de 1998, Pub. L. No. 100-618.

351 Cable Communications Policy Act (CCPA ou « Cable Act »), 1984, Pub. L. No. 98-549, 47 U.S.C. / 551(a)(1).

352 En plus du Children's Online Privacy Protection Act et du Electronic Communications Privacy Act, évoqués infra, n° 58-63, cf. le Computer Fraud and Abuse Act (CFAA), de 1984, 18 U.S.C. § 1030.

353 Telephone Consumer Protections Act (TCPA), de 1991, Pub. L. No. 102-243, 47 U.S.C. § 227.

354 Controlling the Assault of Non-Solicited Pornography and Marketing (Can-Spam) Act, de 2003, Pub. L. No. 108-187, 15 U.S.C. § 7701 et s.

56. Le EPCA est formé de trois textes : the *Wiretap Act*, 18 U.S.C. § 2510-2522 qui réglemente l'interception des télécommunications ; le *Stored Communications Act* (SCA), 18 U.S.C. § 2701-2711 qui régule les communications dans le stockage et les fichiers des clients des fournisseurs d'accès Internet ; enfin, le *Pen Register Act*, 18 U.S.C. § 3121-3127 qui réglemente l'utilisation du *pen register*, c'est-à-dire le dispositif qui permet l'interception des données de connexion électronique et téléphonique. Disons-le d'emblée, ces textes n'ont pas permis d'appréhender les impacts possibles du recours massif à la publicité ciblée sur la maîtrise informationnelle et les dangers d'un traitement massif de données personnelles à l'insu des particuliers et consommateurs. Le droit à l'oubli comme droit à l'autodétermination informationnelle est très loin d'être assuré par ces dispositions qui étaient destinées à répondre à des problèmes importants, mais très éloignés de ceux que soulève actuellement l'utilisation commerciale des données.

57. Les rares arrêts disponibles montrent que les deux premiers textes du EPCA présentent de très sérieuses limites y compris face à des comportements qui s'apparentent à de l'espionnage. L'affaire *In re Pharmatrak, Inc. Privacy Litigation*[355], jugée en 2002, en fournit la parfaite illustration. Les faits étaient passablement compliqués, et l'on retiendra que la société Pharmatrack, spécialisée dans la collecte et l'analyse de données, avait conclu un contrat avec plusieurs entreprises pharmaceutiques au terme duquel, sans collecter de données personnelles, la société d'exploration de données se chargerait d'analyser la consultation sur les sites Internet respectif des entreprises cocontractantes. Il s'avéra, par la suite, que Pharmatrak avait pu, au moyen de procédés complexes (dont l'utilisation de cookies traceurs, de pixels invisibles[356] et de programmes et scripts), collecter une grande quantité de données personnelles (y compris certaines données relatives à des courriels), dont le nom, l'adresse, les numéros de téléphone, la date de naissance, le sexe, le statut assurantiel, l'état de santé, le niveau d'éducation et l'activité professionnelle. Les demandeurs – des utilisateurs – alléguaient une violation du titre I du EPCA, à savoir le *Wiretap Act*, dont le texte pertinent dispose que « [à] moins qu'il en soit expressément disposé autrement dans ce chapitre[,] toute personne qui – (a) intentionnellement, intercepte, tente d'intercepter ou procure à toute personne d'intercepter une communication orale, téléphonique ou électronique… sera punie comme indiqué à la sous-section (4) ou sera poursuivi conformément à la sous-section (5) »[357]. Le raisonnement laborieux des premiers juges[358] fut censuré en appel[359] et il n'est pas

---

355 In re Pharmatrak, Inc. Privacy Litigation, 220 F. Supp. 2d 4 (D. Mass. 2002).

356 Un pixel invisible ou « Clear GIF » est une image graphique d'un pixel de côté ou de deux pixels de côté qui est invisible pour l'utilisateur et qui permettait, en l'occurrence, à Pharmatrak de faire communiquer directement le navigateur de l'utilisateur avec ses serveurs.

357 18 U.S.C. § 2511(1)(a).

358 Pour les demandeurs, il ne faisait aucun doute que les entreprises défenderesses avaient intentionnellement « intercepté » leurs communications avec les sites Internet visités, sans leur autorisation ou consentement. Pour les premiers juges, toutefois, l'argument ne pouvait prospérer. Le Wiretap Act prévoit, en effet, une exception importante qui fait échec aux poursuites lorsque la personne qui intercepte est partie à la communication ou lorsque l'une des parties à la communication a donné son consentement préalable à l'interception (18 U.S.C. § 2511(2)(d) : « En vertu du présent chapitre, il n'est pas illégal, pour une personne n'agissant pas sous couvert de la loi, d'intercepter une communication orale, téléphonique ou électronique, lorsque cette personne est partie à la communication ou lorsque l'une des parties a donné son consentement préalable à une telle interception […] »). Or, pour les premiers juges, les entreprises pharmaceutiques avaient accepté que Pharmatrak modifiât le fonctionnement

nécessaire de s'y attarder. On retiendra simplement que, sur renvoi, les juges ont estimé que l'interception n'était pas intentionnelle et que, tout au plus, Pharmatrak avait réuni les données personnelles par négligence[360].

58. Les demandeurs connaîtront le même sort sur le fondement du titre II du ECPA, c'est-à-dire le *Stored Communications Act* (SCA). Là encore, l'objet du texte était très différent de ce que les demandeurs cherchaient à dénoncer. Comme le laisse transparaître la disposition pertinente du texte, la loi avait été adoptée pour lutter contre les hackers qui obtiennent, altèrent ou détruisent certaines communications téléphoniques et électroniques ou des dossiers transactionnels stockés : « Quiconque — (1) accède intentionnellement, sans autorisation, à une installation permettant la fourniture d'un service de communication électronique ; ou (2) outrepasse intentionnellement l'autorisation d'accès à cette installation ; et de cette façon obtient, altère ou empêche l'accès autorisé à une communication téléphonique ou électronique qui est stockée électroniquement dans un tel système sera puni comme indiqué par la sous-section (b) de cette section »[361]. L'argument des demandeurs, selon lequel le dispositif mis en place par Pharmatrak s'apparentait à une véritable intrusion électronique (« *electronic trespassing* »), tombant purement et simplement sous le coup de la section 2701 du texte précité, est assez logiquement rejetée : bien que les ordinateurs et téléphones fournissent certainement des services, au sens général du mot, il ne s'agit certainement pas d'un service d'accès à Internet[362], service qui est fourni par des fournisseurs d'accès à Internet et non par des ordinateurs personnels.

59. Admettons, d'ailleurs, qu'il en soit autrement, c'est-à-dire que les ordinateurs individuels soient tenus pour une *installation permettant la fourniture d'un service de communication électronique*, que la protection des données personnelles des internautes ne s'en trouverait pas mieux assurée. L'affaire *In re Doubleclick Inc. Privacy Litigation*[363] montre une autre limite du texte. Les faits étaient simples : l'entreprise *DoubleClick*, régie publicitaire aujourd'hui propriété de Google, utilisait (et utilise encore) des cookies pour recueillir des données sur les internautes de manière à permettre, ensuite, la pratique de la publicité comportementale. Le même article du SCA était débattu (18 U.S.C. § 2701(a)), mais la juridiction adopte cette fois-ci un raisonnement différent : l'ordinateur individuel de l'internaute, une fois connecté à Internet, devient une « installation permettant la fourniture d'un service de communication électronique ». Le texte reçoit donc application – même si c'est au prix d'une déformation complète du texte[364] –, mais sans pour autant que soit réservé un sort meilleur à l'internaute. C'est que le § 2701(c)(2) prévoit une exception consistant

---

de leur site Internet, et leur consentement faisait directement obstacle à l'action sur le fondement du Wiretap Act. Comme, du reste, les entreprises défenderesses étaient contractuellement liées à Pharmatrak et l'avaient autorisée à communiquer avec tout utilisateur qui entrait en communication avec l'un des sites Internet, elles étaient partie à la communication avec les demandeurs.

359 In Re Pharmatrak, Inc. Privacy Litigation, 392 F.3d 9 (1st Cir. 2003).

360 In re Pharmatrak, Inc. Privacy Litigation, 292 F. Supp. 2d 263 (D. Mass. 2003).

361 18 U.S.C. § 2701(a).

362 Un service de communication électronique est « tout service qui fournit aux utilisateurs de celui-ci l'aptitude à envoyer ou recevoir des communications téléphoniques ou électroniques » (18 U.S.C. § 2510(15).

363 In re Doubleclick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

364 O.S. Kerr, « Lifting the "Fog" of Internet Surveillance : How a Suppression Remedy Would Change Computer Crime Law », 54 Hasting L.J. 805 (2003), p. 831.

dans la « conduite autorisée [...] par un utilisateur de ce service concernant la communication qu'il émet ou qui lui est destinée ». Certes, les internautes n'avaient évidemment pas consenti, mais les sites Internet qui utilisaient les cookies de *DoubleClick* étaient, selon la juridiction, eux aussi des utilisateurs et avaient bel et bien consenti. Leur seul consentement était suffisant.

60. Dans la gamme des pratiques qui mettent également en péril l'autodétermination informationnelle et qui plaident aujourd'hui en faveur d'un droit à l'oubli en tant que meilleure maîtrise de ses données personnelles, figure également la question de la divulgation d'informations à des tiers. Dans l'affaire *Dyer v. Northwest Airlines Corp*[365], par exemple, était discutée la pratique mise en place après les attentats du 11 septembre et consistant pour la *National Aeronautics and Space Administration* (NASA) à demander aux compagnies aériennes la transmission de données de systèmes sur les passagers, pendant une certaine période, afin de conduire des études sur la sécurité aérienne. La compagnie *Northwest Airlines* avait déféré à l'une de ces demandes et divulgué, en conséquence, et secrètement, des informations telles que le nom, l'adresse, le numéro de carte de crédit et l'itinéraire des personnes qui avaient voyagé sur la compagnie entre juillet et décembre 2001. Huit actions de groupe avaient été introduites contre la compagnie aérienne et il revenait à la juridiction de statuer sur la violation alléguée de l'ECPA, en particulier de cette disposition faisant interdiction à une personne ou entité fournissant soit un service de communication électronique ou un service informatique à distance au public de « divulguer, en connaissance de cause, un dossier ou tout autre information concernant un abonné ou un client dudit service... à une quelconque entité gouvernementale »[366]. Mais, comme le rappelle la juridiction, une entreprise qui vend des biens ou services sur Internet est à distinguer d'une entreprise qui fournit un accès à Internet[367], la seule qui relève du § 2702(a)(3) du texte précité. Or l'entreprise *Northwest Airlines* ne vend que des billets d'avion sur son site Internet, en aucun cas des services Internet. Elle se trouve donc hors du champ d'application de l'ECPA et aucune autre disposition ne faisait obstacle à la divulgation des registres passagers.

61. Il n'est véritablement qu'un texte qui témoigne du souci réel d'une garantie effective de l'autodétermination informationnelle sur l'Internet et qui assure, en certaines circonstances, l'effacement des données et donc une forme de droit à l'oubli. Mais la nature protectrice du texte s'explique par la faiblesse particulière de ceux qui en sont les sujets, à savoir les mineurs. Il s'agit en effet du *Children's Online Privacy Protection Act*[368] (COPPA), adopté en 1998, qui réglemente la collecte et l'utilisation, par les sites Internet, des données personnelles des mineurs qui ont moins de 13 ans[369]. Le texte s'applique « à l'exploitant d'un site Internet ou d'un service en ligne destiné aux enfants, ou tout exploitant qui a une connaissance réelle de ce qu'il collecte des données personnelles auprès d'un mineur »[370]. Fondé sur le principe du *notice-and-choice* (notification et avis), dont on verra les conséquences qu'y attache la *Federal Trade Commission*[371], le texte exige que les

---

365 Dyer v. Northwest Airlines Corp. 334 F. Supp. 2d 1196 (D.N.D. 2004).

366 18 U.S.C. § 2702(a)(3).

367 La juridiction se fonde sur In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

368 Pub. L. No. 106-170, 15 U.S.C. § 6501-6506.

369 15 U.S.C. § 6502(1).

370 15 U.S.C. § 6502(a)(1).

371 V. infra, n° 75 et s.

sites Internet destinés aux enfants mettent en ligne leur politique en matière de vie privée, en décrivant « quelles sont les informations collectées auprès de l'enfant par l'exploitant, comment l'exploitant utilise ces informations, et les pratiques de l'exploitant en matière de divulgation de ces informations »[372]. Voilà la notification. Quant au consentement, le texte précise que les sites destinés aux mineurs doivent « obtenir le consentement vérifiable des parents pour la collecte, l'utilisation ou la divulgation des informations personnelles obtenues du mineur »[373]. On retrouve ensuite les principales composantes de ce qui formerait un droit à l'oubli : principe de finalité, droit à la désidentification ou à la suppression des données ou bien droit à d'opposition à une collecte ultérieure de données. Le texte dispose en effet que l'opérateur doit fournir aux parents une description « du type spécifique d'information personnelle collectée », de manière qu'ils puissent exercer leur droit « de refuser à l'opérateur toute autre utilisation ou le maintien dans une forme récupérable des informations personnelles collectées auprès du mineur ou encore toute autre collecte en ligne d'information personnelle auprès de l'enfant ».

62. L'intervention de la FTC peut également conduire à une forme d'effacement des données. Il faut d'abord comprendre que le COPPA n'ouvre aucun recours individuels et seuls les États peuvent introduire des actions civiles, en tant que *parens patriae*, pour violation du COPPA. Agissant pour le compte du citoyen, l'*attorney general* (procureur général) de l'État peut obtenir en justice l'interdiction de la pratique, la mise en conformité avec le texte, des dommages et intérêts et tout autre mesure que la cour juge appropriée[374]. Mais c'est la FTC qui joue le rôle principal en sanctionnant les politiques de vie privée établies dans le cadre du COPPA ou les lignes directrices d'autorégulation approuvées par la FTC[375], qui constituent, le cas échéant, des pratiques trompeuses ou déloyales. Dans le cadre des procédures déclenchées pour violation du FTCA et du COPPA, qui aboutissent le plus souvent, on le verra, à des transactions (« *settlements* »), la FTC peut prononcer des sanctions particulièrement contraignantes, dont *l'effacement* de toutes les données récolées par un exploitant. Tel fut le cas dans l'affaire *United States v. W3 Innovations, LLC*[376], qui a donné lieu à des poursuites en 2011 et qui s'est terminée par un accord aux termes duquel l'entreprise W3 Innovations, développeur d'applications de jeux iPhone et iPod pour mineurs, s'est engagée à payer une amende de $50 000 et à effacer toutes les informations collectées en violation du COPPA[377].

63. À l'exception des remarques faites sur le COPPA, le constat dressé serait presque désolant s'il n'était pas relevé que, à l'échelle étatique, les législateurs n'ont pas toujours entendu laisser les citoyens complètement désarmés face aux pratiques invasives des entités commerciales

---

372 15 U.S.C. § 6502(b)(1)(A)(i).

373 15 U.S.C. § 6502(b)(1)(A)(ii). Lorsque l'information n'est pas maintenue dans une forme récupérable, le consentement n'est pas requis (§ 6502(b)(2)). Une forme de minimisation des données est également exigée : les sites Internet ne peuvent conditionner la participation d'un mineur à un jeu ou la remise d'un prix à la divulgation de plus d'informations que nécessaire pour participer à l'activité § 6502(b)(1)(C).

374 15 U.S.C. § 6504.

375 Cf. 15 U.S.C. § 6504.

376 United States v. W3 Innovations, LLC, No. CV-11-03958-PSG (Aug. 12, 2011).

377 En l'occurrence, l'entreprise W3 Innovations n'avait établi aucune politique en matière de vie privée et n'avait pas davantage recherché le consentement des parents avant de procéder à la collecte et à la divulgation de données personnelles de mineurs.

et que, à l'échelle fédérale, le Congrès s'est parfois montré soucieux de mieux protéger certaines catégories de données[378]. Il ne faudrait pourtant pas en conclure trop rapidement à la consécration d'une maîtrise informationnelle comparable à celle que l'on cherche à établir en Europe. C'est que le Premier amendement a joué une nouvelle fois le rôle de repoussoir à une protection trop étendue des données personnelles, ce qu'a permis une assimilation du traitement des données à un discours commercial protégé.

B- L'assimilation du traitement des données à un discours commercial protégé

64. Depuis l'arrêt *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.* [379], de 1976, le discours commercial bénéficie d'une protection constitutionnelle. Entendue comme celui qui « propose une transaction commerciale »[380], une « expression liée seulement aux intérêts économiques de l'orateur et de son public »[381], il présente traditionnellement une valeur plus faible que les autres catégories de discours et jouit, partant, d'une protection moins étendue[382]. C'est à l'occasion de l'affaire *Central Hudson* de 1980[383] que la Cour a posé les jalons d'un test en quatre parties pour évaluer la constitutionnalité des restrictions apportées aux discours commerciaux :

> « Au début, nous devons déterminer si l'expression est protégée par le Premier amendement. Pour que le discours commercial relève de cette disposition, il doit pour le moins porter sur une activité légale et ne pas être trompeur. Ensuite, nous nous demandons si l'intérêt gouvernemental allégué est substantiel. Si les deux examens donnent des réponses positives, nous devons déterminer si la réglementation fait directement avancer l'intérêt du gouvernement, et s'il ne va pas au-delà de ce qui est nécessaire pour servir cet intérêt ».

La Cour Suprême a plus tard révisé la dernière partie du test : la réglementation doit assurer « un ajustement <*fit*> entre les finalités du législateurs et les moyens choisis pour atteindre ces finalités,... un ajustement qui n'est pas nécessairement parfait, mais raisonnable »[384].

65. C'est sur ce fondement que la Cour Suprême et plus largement les juridictions se sont efforcées, dans le domaine commercial, de concilier liberté d'expression et protection de la vie privée et des données personnelles. L'examen de la jurisprudence paraît reposer sur deux principes organisationnels : l'antique principe de *common law* qui offre une protection absolu au domicile et à la propriété ; le principe utilitariste de faveur donnée à la solution juridique la plus

---

378 V. infra, n° 73 et s.

379 Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

380 Virginia State Board, op. cit.

381 Central Hudson Gaz & Electric Corp. v. Public Service Comm'n of New York, 447 U.S. 557 (1980).- La Cour Suprême a ultérieurement précisé que ces critères, bien que devant être pris en compte dans la détermination de la nature commerciale d'un discours, ne sont pas toujours déterminants : Bolger v. Youngs Drug Products Corp., 463 U.S. 60 (1983). V. aussi les remarques de E. Volokh, « Freedom of Speech and Information Privacy : The Troubling Implications of a Right to Stop People from Speaking About you », op. cit., spéc. p. 1082 (qui expliquent bien le phénomène de renforcement de la protection des « discours commerciaux » décrit au texte).

382 Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447 (1978).

383 Central Hudson Gaz & Electric Corp. v. Public Service Comm'n of New York, op. cit.

384 Board of Trustees of State University of New York v. Fox, 492 U.S. 469 (1989).

efficiente sur le plan économique. Le premier se donne à voir sans peine dans deux arrêts relatifs à la prospection commerciale. L'arrêt *Rowan v. United States Post Office Department*[385], rendu en 1970 par la Cour Suprême, mettait en débat la constitutionnalité d'une loi fédérale autorisant les individus à exiger des entités recourant à la prospection commerciale par voie postale de retirer leur nom des listes d'adresse et de mettre un terme aux démarchages. Tout en reconnaissant que, dans nos sociétés modernes et complexes, l'individu est devenu un auditeur continuellement sollicité et à des fins multiples, elle n'en soulignait pas moins qu'une « mesure suffisante d'autonomie individuelle [doit] survivre pour permettre à chaque propriétaire <*householder*> d'exercer un contrôle sur le courrier indésirable ». La référence à l'autonomie individuelle fait signe vers les droits continentaux de la personnalité, mais la trajectoire transatlantique achoppe sur la conception domiciliaire qu'impose l'histoire du droit américaine. Aussi la Cour reprend-elle, à maintes reprises, ce langage inaltéré depuis le *Semayne's Case* dont elle extrait d'ailleurs la formule-étendard (« *a man's home is his castle* », dans lequel « même pas le roi ne peut entrer »)[386] : le propriétaire est juge exclusif et ultime de ce qui est autorisé à passer le « seuil » de sa maison. Rien d'étonnant alors à ce qu'elle fasse également référence au *tort* de *trespass*, en rappelant qu'elle « a traditionnellement respecté le droit du propriétaire d'interdire, par ordonnance ou avis, l'accès à sa propriété à des démarcheurs, des colporteurs et des marchands ambulants ». La disposition fédérale contestée était aussi bien conforme à la Constitution, car « [r]ien dans la Constitution ne nous oblige à écouter ou à regarder une communication non désirée, quel qu'en soit le mérite ».

66. La conclusion est comparable et s'adosse surtout sur les mêmes motifs dans le second arrêt, rendu dans l'affaire *Mainstream Marketing Services, Inc. v. Federal Trade Commission*, par une juridiction d'appel du 10e circuit[387]. En 2003, deux agences fédérales – la Federal Trade Commission (FTC) et la Federal Communications Commission (FCC) – promulguaient un ensemble de règles donnant naissance au *do-not-call registry*, c'est-à-dire une liste d'opposition comparable à la liste française PACITEL (« liste orange »)[388], mentionnant les numéros de téléphone d'abonnés téléphoniques ayant volontairement fait le choix de ne plus recevoir de sollicitations commerciales[389]. La constitutionnalité des règles adoptées par la FCC étaient contestée devant la juridiction fédérale. Il n'est pas sans intérêt de remarquer que cette liste orange était le résultat d'efforts remontant à 1991 et destinés à protéger la vie privée des consommateurs et les risques d'abus du télémarketing. Dans le *Telephone Consumer Protection Act* de 1991 (TCPA) – dans le cadre duquel les dispositions réglementaires de la FCC ont été adoptées – le Congrès avait bien insisté sur le fait que, pour nombre de consommateurs, le télémarketing constituait une immixtion dans leur vie privée. D'où ce premier intérêt avancé par l'État à l'appui de cette législation : la protection de la vie des individus à leur domicile ; intérêt auquel vient s'ajouter la protection des individus contre le risque de sollicitations abusives et frauduleuses.

---

385 Rowan v. United States Post Office Department, 397 U.S. 728 (1970).

386 V. supra, n° 18.

387 Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F.3d 1228 (10th Cir. 2004).

388 16 C.F.R. § 310.4(b)(1)(iii)(B)(règles de la FTC) ; 47 C.F.R. § 64.1200(c)(2) (règles de la FCC).

389 Il faut préciser que le texte ne s'appliquait qu'aux appels passés par des vendeurs de biens ou services ou au nom de ceux-ci ; mais en aucun cas aux démarchages téléphoniques destinés à collecter des fonds de bienfaisance ou politiques. Un vendeur pouvait du reste solliciter des consommateurs figurant sur la liste en justifiant soit d'une relation commerciale établie avec le consommateur, soit du consentement écrit de ce dernier.

Voilà deux intérêts qui, pour la juridiction, sont substantiels au sens du test *Central Hudson*. L'intérêt du raisonnement se trouve cependant ailleurs. En premier lieu, le motif qui vient soutenir le caractère substantiel est, à travers une référence appuyée à *Rowan*, directement extrait de l'affaire *Semayne*. On le voit avec une netteté particulière lorsque la juridiction se réclame de cet autre précédent de la Cour Suprême, *Frisby v. Schultz*, qui date de 1988[390] : « L'un des avantages particuliers de la vie privée dont tous les citoyens peuvent jouir entre leurs propres murs, que l'État doit s'attacher à protéger légalement, est l'aptitude à éviter les intrusions ». C'est parce que la législation fédérale entend protéger le domicile et son enceinte que la législation fédérale et la réglementation en cause bénéficient d'une sorte de présomption de constitutionnalité. En second lieu, c'est l'examen du mécanisme d'*opt-in* mis en place par la réglementation, vivement critiquée dans un arrêt antérieur d'une autre cour d'appel du 10e circuit[391], qui mérite l'attention. Dans le cadre du contrôle intermédiaire (« *intermediate scrutiny* »), qui gouverne normalement[392] le contrôle de constitutionnalité des lois limitant les discours commerciaux, aucun examen de *nécessité*[393] n'est à proprement parler exercé. Si l'existence d'« alternatives nombreuses et évidentes, moins lourdes »[394] est à prendre en compte, les juges n'ont pas à rechercher, comme en droit allemand, « si d'autres moyens appropriés affectant de façon moins préjudiciable la personne concernée et la collectivité ne sont pas à la disposition de l'autorité »[395]. L'essentiel est que la réglementation soit « strictement adaptée » (« *narrowly tailored* ») et qu'existe un ajustement raisonnable entre le problème et la solution adoptée. La position du législateur est là encore favorisée, car il lui suffit de montrer que le mécanisme juridique pour lequel il a opté (en l'occurrence l'*opt-in*) est moins restrictif que celui qui aboutirait à interdire directement une forme de discours.

67. Lorsqu'on s'écarte de cette tour de verre que forme le domicile, les juridictions, qui utilisent pourtant le même cadre conceptuel, se montrent apparemment plus rigoureuses. Un arrêt antérieur à celui qui vient d'être mentionné, rendu également par une cour d'appel du 10e circuit, en témoigne sans ambiguïté. L'affaire *U.S. West, Inc. v. Federal Communications Commission*[396] concernait une réglementation[397] adoptée par la *Federal Communications Commission* restreignant l'usage et la divulgation des « informations de réseau exclusives sur les clients » (« *Customer Proprietary Network Information* » ou CPNI)[398], ainsi que l'accès à celles-ci. Les dispositions

---

390 Frisby v. Schultz, 487 U.S. 474 (1988).

391 V. infra, n° 67 : U.S. West, Inc. v. Federal Communications Commission, 182 F.3d 1224 (10th Cir. 1999).

392 Cette question est débattue : v. infra, n° 69.

393 Cf. E.Th. Sullivan, R.S. Frase, Proportionality Principles in American Law.- Controlling Excessive Government Actions, Oxford University Press, Oxford, New York, 2009, spéc. p. 59 qui remarquent que, à la différence du contrôle de proportionnalité qui est réalisée par la Cour Suprême allemande ou la CEDH, le contrôle intermédiaire américain n'implique pas une stricte nécessité, c'est-à-dire la démonstration de ce que la mesure choisie était l'ultima ratio (cf. Turner Broadcasting System, Inc.. v. F.C.C., 512 U.S. 622 (1994), spéc. p. 662). En réalité, le test de l'ultima ratio est réalisé dans le cadre du contrôle strict (v. supra, n° 21).

394 Mainstream Marketing Services, Inc., op. cit.

395 H. Maurer, Droit administratif allemand, (trad. M. Fromont), LGDJ, Paris, 1995, p. 272.

396 U.S. West, Inc. v. Federal Communications Commission, 182 F.3d 1224 (10th Cir. 1999).

397 63 Fed. Reg. 20,326 (1998) (« CPI Order »).

398 « L'expression "informations de réseau exclusives sur les clients" (customer proprietary network information) désigne les informations concernant "le nombre, la configuration technique, le type, la destination et la fréquence d'utilisation des services de télécommunications" fournis à un client ainsi que les informations contenues dans les

réglementaires de la FCC portaient sur le paragraphe 222 du titre 47 de l'United States Code[399] qui forme une partie du *Telecommunications Act* de 1996. Le paragraphe 222, intitulé « Confidentialité <*Privacy*> des informations de consommateur », énonce que « tout opérateur de télécommunications a l'obligation de protéger la confidentialité des informations exclusives sur les clients ou en rapport avec les clients ». La disposition centrale était le § 222(c)(1) qui dispose que « [à] moins que la loi n'en dispose autrement ou sauf consentement du client, un opérateur de télécommunications qui reçoit ou obtient des informations de réseau exclusives sur les clients en raison de la fourniture d'un service de télécommunication doit seulement utiliser, divulguer ou permettre l'accès à ces informations de réseau exclusives sur des clients individuellement identifiables dans la production (A) du service de télécommunications dont l'information est issue, ou (B) des services nécessaires à la fourniture d'un tel service de télécommunications ou utilisés dans le cadre de cette fourniture, y compris la production des annuaires ». En plus de l'exception liminaire tirée du consentement, le § 222(d) prévoit trois exceptions additionnelles qui permettent aux entreprises concernées, respectivement d'utiliser et de divulguer les informations de réseau exclusives sur les clients à des fins de facturation, de prévention des fraudes et de fourniture de services au consommateur, si le consommateur consent à l'usage de l'information à cette fin. L'enjeu portait sur l'expression du consentement, en particulier celui exigé par le § 222(c)(1) : suffisait-il que le consommateur ne s'oppose pas (mécanisme de l'*opt-out*) ou fallait-il qu'il donne expressément son accord et qu'il soit donc recherché par l'opérateur (mécanisme de l'*opt-in*) ? C'est à cette dernière branche de l'alternative que s'était rangée la FCC et dont U.S. West contestait la constitutionnalité.

68. Ce choix n'a pas convaincu la cour qui s'est montrée particulièrement rigoureuse à chacune des étapes du contrôle. Rigueur qui apparaît déjà dans l'examen des intérêts avancés par le Gouvernement, en l'occurrence la protection de la vie privée des consommateurs et la promotion de la concurrence. Protéger la vie privée est sans doute un objectif louable, reconnaît la juridiction, mais le Gouvernement « doit préciser la notion particulière de vie privée et l'intérêt servi ». On voit surtout poindre les effets de la rationalité économique : « Au surplus, la vie privée n'est pas un bien absolu parce qu'il impose des coûts réels à la société ». Rigueur qui est également perceptible dans la reformulation presque insensible du deuxième critère de contrôle : il n'est plus seulement dit que la réglementation doit faire directement avancer l'intérêt de l'État, mais qu'elle doit le faire directement et substantiellement/dans une grande mesure (« *materially* »). Or cela change beaucoup de choses dans l'appréciation du préjudice que l'État entend défendre à travers sa réglementation. Il ne suffit plus de raisonner dans l'abstrait sur les conséquences de telle ou telle divulgation, mais il faut montrer que « la dissémination des informations que l'on souhaite tenir secrètes infligerait aux individus un préjudice réel et significatif, tel qu'une gêne excessive ou une raillerie, de l'intimidation ou du harcèlement, ou bien encore le détournement d'informations personnelles sensibles afin d'endosser l'identité d'autrui ». La rigueur transparaît

---

factures de téléphone [47 USC, § 222 f) 1)]. Elle n'englobe toutefois pas les informations relatives à la liste des abonnés (idem) », Commission, Décision de la Commission du 26 juill. 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, (2000/520/CE), JOCE 25.8.2000 L 215/7.

399 47 U.S.C. § 222.

enfin à travers le troisième critère, celui de l'ajustement entre fins et moyens. On a pu voir que la jurisprudence attachait quelque importance à l'existence d'« alternatives nombreuses et évidentes, moins lourdes »[400]. Ce critère est normalement moins exigeant que celui mis en œuvre dans le cadre d'un contrôle strict de nécessité. Et pourtant, la Cour examine soigneusement l'existence d'autres voies de droit, à l'occurrence le recours à un mécanisme d'*opt-out*. L'ensemble de l'arrêt, qui a conduit en l'occurrence à une décision d'inconstitutionnalité, a été vivement critiquée par l'opinion dissidente de Briscoe, qui a souligné que le mécanisme de l'*opt-in* était le seul à garantir un consentement réel du consommateur. D'ailleurs, la FCC, dans son ordonnance de 2007[401], a maintenu le mécanisme d'*opt-in* en cas de partage d'informations entre membres d'une société en participation (*joint venture*) ou avec des entrepreneurs indépendants. D'une manière générale, notait la FCC, la fausseté des prémisses sur lesquelles avaient été fondées la décision *U.S. West* a été démontrée. Des preuves substantielles ont permis d'établir qu'un mécanisme d'*opt-out* ne protégeait pas suffisamment la vie privée des consommateurs, soit qu'ils ne lisent pas, soit qu'ils ne comprennent les politiques en matière de vie privée des opérateurs[402]. Une juridiction du district de Columbia lui a du reste plus tard donné raison sur ce point[403].

69. Les espoirs qu'ont pu susciter les prolongements de l'affaire *U.S. West* paraissent avoir été déçues par l'arrêt *Sorrell v. IMS Health, Inc*, de 2011[404], qui montre, une nouvelle fois, que la protection offerte à la vie privée doit s'incliner devant le Premier amendement, chaque fois que le domicile n'est pas affecté et se trouvent en jeu des intérêts économiques dont le bénéfice attendu surpasse celui qu'offre la protection de la vie privée dans une perspective de maximisation du bien-être de la communauté. Une loi de l'État du Vermont, adoptée en 2007, restreignait, en l'occurrence, la vente, la divulgation et l'utilisation de dossiers pharmaceutiques enregistrant les pratiques de prescription des médecins[405]. Sauf exceptions, l'information ne pouvait vendue,

---

400 V. supra, n° 66.

401 FCC Report and Order, 07-22 (April 2, 2007).

402 V. aussi, favorable à un mécanisme d'opt-in, J. Sovern, « Opting in, Opting Out, or No Options at All : The Fight for Control of Personal Information », 74 Wash. L. Rev. 1033 (1999).- Contra, M.E. Staten, F.H. Cate, « The Impact of Opt-in Privacy Rules on Retail Markets : A Case Study of MBNA », 52 Duke L.J. 745 (2003), p. 750-51, 770-774, 776

403 National Cable and Telecommunications Association, 555 F.3d 996 (D.C. Cir. 2009). La juridiction a jugé que le gouvernement avait un intérêt substantiel dans la « protection de la vie privée des informations de crédit du consommateur ». Elle a pareillement estimé que l'ordonnance de 2007 « faisait directement avancer » l'intérêt du gouvernement : « Le sens commun soutient la conclusion de la Commission selon laquelle le risque de divulgation non autorisée d'informations sur le client augmente avec le nombre d'entités qui les possèdent. La Commission en conclut du reste raisonnablement qu'une exigence de consentement par opt-in a fait directement et concrètement avancer l'intérêt en protégeant la vie privée du client et en donnant au client un contrôle sur l'information ». Enfin, pour la juridiction, le rapport entre les moyens et le but était proportionné. C'est que, selon elle, la différence entre opt-in et opt-out restait marginale. Et de conclure que l'approche consistant à privilégier l'opt-in était raisonnable.

404 Sorrell v. IMS Health, Inc. 131 S. Ct. 2653 (2011).

405 Vt. Stat. Ann., Tit. 18, § 4631.- Il s'agit de la Prescription Confidentiality Law, également appelée Act 80. Selon la disposition principale, contenue au § 4631(d) : « Une compagnie d'assurance santé, un employeur auto-assuré, un intermédiaire de transmission électronique, une pharmacie ou tout autre entité équivalente ne doit pas vendre, louer ou échanger contre un bien les dossiers réglementés contenant des données identifiantes de prescription <prescriber-identifiable information>, pas plus qu'il ne doit autoriser l'usage de ces dossiers réglementés à des fins de commercialisation ou de promotion de la prescription d'un médicament, sauf consentement du prescripteur… Les

divulguée par les pharmacies à des fins de marketing ou utilisée par l'industrie pharmaceutique à ces mêmes fins. Pour le législateur de l'État, ces interdictions étaient destinées à protéger la confidentialité des données médicales et limiter le risque de prescriptions qui ne soient plus dans l'intérêt des patients ou de l'État. Mais pour la Cour, la disposition litigieuse discrimine selon le contenu du discours et les catégories de locuteurs. En vertu d'une exception prévue au texte, tous ceux qui souhaitent s'engager dans des « communications éducatives » (§ 4621(e)(4)) peuvent acheter l'information ; ce qui ne fait que confirmer que la disposition défavorise la commercialisation, c'est-à-dire une forme de discours avec un contenu spécifique. Par ailleurs, la loi défavorise certaines catégories de locuteurs, à savoir les fabricants de médicaments. En d'autres termes, la loi établit des restrictions *qui sont fondées sur le locuteur et le contenu du discours*, ce qui justifie la mise en place d'un « *heightened judicial scrutiny* », c'est-à-dire d'un contrôle judiciaire renforcé[406]. Préfiguré par l'arrêt *U.S. West*, ce type de contrôle conduit la Cour à examiner avec la plus grande rigueur chacune des conditions exigées par son test en trois parties.

70. Il n'est presque pas besoin de détailler le raisonnement de la Cour, tant ses délinéaments excessivement défavorables à l'État sont prévisibles, comme l'est du reste la conclusion : une violation du Premier amendement. Les intérêts avancés par l'État sont louables : protéger la confidentialité des données médicales, lutter contre le harcèlement et préserver l'intégrité de la relation médecin-patient ; de même qu'améliorer la santé publique et, surtout, réduire les coûts des frais de santé (ce que la législation réalise concrètement en permettant à l'État du Vermont de fournir à des institutions académiques des informations identifiantes de manière à contrer le message commercial de l'industrie pharmaceutiques qui chercherait à promouvoir ses marques au détriment des médicaments génériques). Mais l'État aurait pu garantir la confidentialité des données relatives au médecin à travers une « réglementation plus cohérente »[407], en particulier en autorisant la divulgation et la vente des données dans des circonstances à la fois plus étroites et mieux justifiées. C'est que, note la Cour Suprême, la loi contestée du Vermont mettait les informations relatives aux pratiques de prescription à disposition d'un nombre presque illimité de personne. Cette large disponibilité de l'information ne justifiait donc que fût placé un fardeau aussi lourd sur les pharmaciens et l'industrie pharmaceutique en général. Mais l'essentiel réside dans le poids que la Cour accorde aux arguments utilitaristes. Pour les entreprises d'exploration de données et les fabricants de

---

fabricants et distributeurs de produits pharmaceutiques ne doivent pas utiliser les données identifiantes de prescription à des fins de commercialisation ou de promotion de la prescription d'un médicament, sauf consentement du prescripteur ». Le texte habilitait l'Attorney general du Vermont à agir en responsabilité civile et obtenir des dommages intérêts contre les auteurs de violations du texte.

406 Cf. United States v. Playboy Entm't Grp., Inc., 529 U.S. 803, 813 (2000) ; Simon & Schuster, Inc. v. Members of N.Y. State Victims Bd., 502 U.S. 105, 118 (1991). La nature exacte du « heightened judicial test » est controversée. Il ne serait, pour certains, qu'une autre manière de designer le « intermediate scrutiny test ». En réalité, comme a pu le montrer l'arrêt Witt v. Department of the Air Force (527 F.3d 806 (9th Cir. 2008)), rendu dans un autre contexte, et les arrêts cités au texte, le « contrôle judiciaire renforcé » paraît s'intercaler entre le contrôle strict et le contrôle intermédiaire.

407 Formule tirée de Greater New Orleans Broadcasting, 527 U.S. 173, (1999), spéc. p. 195.

médicaments, directement visés[408], cette loi remettait en cause les pratiques de « *detailing* », c'est-à-dire de « visite médicale ». La promotion des médicaments repose souvent sur l'activité d'un représentant de commerce – visiteur médical – qui programme une visite au cabinet médical d'un médecin afin de persuader ce dernier, échantillons et études médicales à l'appui, de recourir à la prescription du médicament de l'entreprise qu'il représente. Afin de cibler le discours de leurs visiteurs médicaux, les entreprises pharmaceutiques avaient eu recours aux rapports comportementaux produits par des explorateurs de données à partir des informations récolées quotidiennement, par les pharmacies, sur les habitudes des médecins prescripteurs.

71. C'est précisément le rôle de ces visiteurs médicaux qui retient l'attention de la Cour Suprême. C'est grâce à leur connaissance des pratiques de prescription d'un praticien que les représentants commerciaux de l'industrie pharmaceutiques sont à même d'identifier les médecins qui sont susceptibles d'être intéressés par un médicament en particulier et d'adapter ainsi leur discours commercial. C'est tout un modèle économique que la Cour entend soutenir, notamment lorsqu'elle observe que le processus de visite médical est coûteux et que les entreprises l'utilisent le plus souvent pour faire la publicité de médicaments très rentables de la marque encore protégés par brevets. C'est à ce moment-là que les fabricants de médicaments princeps peuvent espérer un retour sur investissement et non plus tard – au moment de l'expiration du brevet – lorsque les génériques arrivent sur le marché. On comprend donc que, du calcul utilitariste auquel se livre la Cour, se dégage un résultat très défavorable à la vie privée dont le coût excède très largement le bénéfice qu'elle est en mesure d'offrir. Le juge Breyer, auteur de l'opinion dissidente (à laquelle se sont joints les juges Ginsburg et Kagan), a vu juste en plaçant l'arrêt de la Cour sous l'ascendant de *Lochner v. New York* de 1905[409], qui ouvre l'ère dite « Lochner », marquée par une farouche opposition de la Cour Suprême à toute loi réglementant les secteurs économiques, en particulier le droit du travail. Cette période atteignit son apogée avec la mise en place du *New Deal* qui donna lieu à une si vive résistance de la Cour que Roosevelt en vint en concevoir un projet de réforme. Comme le note fort justement Breyer : « [...] étant donné la quantité d'initiatives réglementaires qui touchent à des messages commerciaux, la conception de la Cour de sa mission de contrôle menace de nous ramener à une époque heureusement révolue où les juges examinaient avec une grande minutie la législation pour son atteinte à la liberté économique ». Et de conclure sur un avertissement : « L'histoire montre que ce pouvoir a fait l'objet de beaucoup d'abus et a conduit à la constitutionnalisation des théories économiques qui avaient la préférence de ces juristes »[410].

---

408 Brief for the Vermont Medical Society, the New Hampshire Medical Society, the Maine Medical Association, the Medical Association of Georgia, the American Academy of Family Practitioners and the American Academy of Pediatrics as Amici Curiae Supporting Petitioners, No. 10-779, p. 1-2 (http://www.vtmd.org/webfm_send/61).

409 Lochner v. New York, 198 U.S. 45 (1905).

410 V. aussi, pour une opinion comparable, N.M. Richards, « Reconciling Data Privacy and the First Amendment », 52 UCLA L. Rev. 1149 (2005) : « Il y a des parallèles assez nombreux entre la conception traditionnelle de Lochner et la critique des lois sur la protection des données personnelles fondée sur le Premier amendement. Les deux théories sont des réponses judiciaires à des appels en faveur d'une régulation juridique des fractures économiques et sociales provoquées par des changements technologiques rapides. Le Lochnerisme entendait régler un problème socio-technologique majeur de l'ère industrielle – la différence de pouvoir entre les individus et les entreprises dans les conditions de travail au sein de l'industrie ; tandis que la critique tirée du Premier amendement est dirigée contre un problème socio-technologique majeur de notre société de l'information – la différence de pouvoir entre les individus

72. Depuis l'arrêt *Sorrell*, le périmètre de protection de la vie privée face aux stratégies commerciales de traitement de données personnelles paraît s'être réduit comme peau de chagrin. En donnant préséance au critère économique, la Cour Suprême paraît menacer directement l'équilibre de certains textes, comme le *Fair Credit Reporting Act* de 1970 (FCRA)[411], qui encadre l'activité des entreprises spécialisées dans le traitement de données de crédits de consommateurs. Dans l'affaire *Trans Union Corp. v. Federal Trade Commission*, datant de 2001, une juridiction du district de Columbia pouvait encore juger que les dispositions du *FCRA* encadrant les « listes de solvabilité » (« *rapports de solvabilité* »), n'étaient pas contraires au Premier amendement, en particulier parce que ces dossiers de solvabilité, ne servant aucune question « d'intérêt public », ne méritaient qu'une protection constitutionnelle limitée[412]. Même si la protection des discours commerciaux peut se comprendre, on peut rester sceptique face à la proposition selon laquelle les informations ou données personnelles sont des *discours commerciaux*[413]. La question est assurément complexe : il est en réalité sans doute impossible de déterminer, hors de tout contexte, en s'attachant à sa seule nature, si l'information litigieuse peut recevoir la qualification de « discours ». Ce qui permet de trancher est l'*usage* réservé à l'information qui devrait s'accorder avec la finalité du Premier amendement, à savoir *la libre communication des idées* (en particulier par la presse). Daniel Solove a exactement souligné que « plutôt que de se concentrer sur la distinction entre discours et non-discours, la détermination des types d'information à réglementer devrait se focaliser sur des considérations d'ordre politique »[414]. Et Neil Richards a ajouté, même si la finalité qu'il paraît assigner un Premier amendement est beaucoup trop étroite, que « [d]u point de vue du premier Amendement, les sociétés spécialisées dans les bases de données, qui opèrent sur le marché des données personnelles, ne remplissent pas une fonction sociale équivalente à celle, fondamentale, [de dissémination de l'information par la presse] »[415]. Si on accepte ces prémisses[416], deux solutions sont alors possibles : développer une approche catégorielle

---

et les entreprises à l'égard des informations au sein de l'environnement électronique. Les deux théories recouvrent la Constitution d'un vernis libertarien, interprétant cette dernière comme imposant soit "la liberté contractuelle", soit la "liberté de l'information". Les deux théories cherchent à imposer certaines formes de réglementation économique par-delà le pouvoir reconnu aux législateurs. Et les deux théories sont instamment défendues par les entreprises désireuses de se prémunir contre une réglementation placée sous l'égide de principes constitutionnels. Dans la mesure où la critique du Premier amendement est comparable à la vision traditionnelle de Lochner, alors son élévation au rang de droit économique de premier ordre est également douteuse » (cité in D. Solove, P. Schwartz, op. cit., p. 926).

411 15 U.S.C. § 1681, 1681a-1681u.

412 V. aussi, par la suite, Trans Union v. FTC, 295 F.3d 42 (D.C. Cir. 2002) (Trans Union II).

413 Cf. N.M. Richards, Intellectual Privacy, Oxford University Press, 2014 (à paraître), Chapter V.

414 D.J. Solove, « The Virtues of Knowing Less : Justifying Privacy Protections Against Disclosure », op. cit., spéc. p. 979-980.

415 N.M. Richards, « Reconciling Data Privacy and the First Amendment », op. cit., p. 1190.

416 Certains juridictions ont tranché la difficulté en considérant que les informations en jeu s'apparentaient non pas à un discours, mais à une « conduite » : v., en ce sens, les exemples données par A. Bhagwat, op. cit., note (68), p. 864-865 et en particulier IMS Health Inc. v. Ayotte, 550 F.3d 42, (1st Cir. 2008), spéc. p. 52-53, affaire qui concernait une loi, tout à fait comparable à celle débattue dans l'arrêt Sorrell, adoptée par l'État du New Hampshire (N.H. Rev. Stat. Ann. § 318:47-f).

(« *categorial balancing* »)[417] et maintenir ces formes de « discours » commerciaux de faible valeur sous un régime de contrôle de constitutionnalité léger[418] ; ou bien exclure purement et simplement ces traitements de données du champ du Premier amendement[419]. En l'état, quoi qu'il en soit, le droit américain reste très peu protecteur des données personnelles collectées, traitées et transférées dans un cadre commercial et l'on voit mal comment il pourrait s'accommoder d'une forme de droit à l'oubli. Mais avant de pouvoir livrer un diagnostic complet, il faut examiner le rôle de plus en plus important reconnu à la *Federal Trade Commission* dans la protection de la vie privée informationnelle.

II- Le rôle complémentaire et grandissant de la Federal Trade Commission

73. Confrontée à une protection sectorielle et largement ineffective, la *Federal Trade Commission* (FTC), dont le rôle a été progressivement accru, a joué un rôle fondamental, ces dix dernières années, dans la protection effective des données, pour le moins dans les secteurs relevant de sa compétence. Rien ne destinait pourtant la FTC, simple agence chargée de la libre concurrence, à occuper cette place éminente qu'on n'hésite désormais plus à lui reconnaître de véritable agence de protection des données[420].
C'est, en effet, à la faveur d'extensions constantes de sa compétence (A) que la FTC est devenue gardienne de la vie privée informationnelle (B).

A- Les extensions constantes de compétence de la FTC

74. Créée par le *Federal Trade Commission Act* de 1914[421], en même temps que le *Clayton Act*, premier texte américain en matière de pratiques anti-concurrentielles[422], la FTC était initialement un *bureau of competition*, c'est-à-dire une sorte d'autorité de la concurrence. Le contraste est évidemment très fort avec le rôle que la commission se reconnaît aujourd'hui, à savoir la protection du consommateur[423]. Ce changement est dû à une révision de la section 5 du FTCA, de 1938, qui a ajouté à sa compétence initiale en matière de lutte contre les « méthodes de concurrence déloyales » (« *unfair methods of competition* »), celle d'interdiction « des actes et pratiques trompeuses ou déloyales »[424]. Mais il a fallu attendre quelques décennies pour que cette révision

---

417 V. supra, n° 21 pour une définition. Mais comme l'a remarqué un auteur, la Cour Suprême se montre très peu favorable à une approche catégorielle : v. A. Bhagwat, « Sorrel v. IMS Health : Details, Detailing and the Death of Privacy », 36 Vermont Law Review 855 (2012), spéc. p. 863-864.

418 Solution qui a la faveur de D. Solove

419 Solution qui est défendue par N. Richards, qui trouve la précédente décision bien trop modérée.

420 S. Hetcher, « The De Facto Federal Privacy Commission », 19 J. Marshall J. Computer & Info. L. 109 (2000), spéc. p. 131 ; D.J. Solove, W. Hartzog, « The FTC and the New Common Law of Privacy », UC Berkeley Public Law Research Paper No. 2271442 (à paraître in 102 California Law Review (2014)), spéc. p. 11.

421 FTCA, Pub. L. No. 63-203, 38 Stat. 717.

422 Clayton Antitrust Act de 1914, Pub. L. No. 63-212, 38 Stat. 730 - aujourd'hui, codifié, tel qu'amendé, in 15 U.S.C. § 12-27 (2006) et 29 U.S.C. §52-53 (2006).

423 V. sur son site Internet : http://www.ftc.gov/ftc/about.shtm.

424 H.R. Rep. No. 75-1613, p. 2-3 (1937) : « [T]his amendment makes the consumer, who may be injured by an unfair trade practice, of equal concern, before the law, with the merchant or manufacturer injured by the unfair methods of a dishonest competitor ». Et v. aussi : FTC v. Sperry & Hutchinson Co., 405 U.S. 233 (1972), spéc. p. 244 : « The amendment added the phrase "unfair or deceptive acts or practices" to the section's original ban on

montre toutes ses virtualités. Entretemps, le Congrès a amorcé la compétence de la FTC dans le domaine des données personnelles. Il le fit tout d'abord en 1970, en donnant autorité à la FTC pour assurer l'exécution du *Fair Credit Reporting Act* (FCRA)[425], puis en 1998, en lui reconnaissant un pouvoir réglementaire et d'exécution dans le cadre du *Children's Online Privacy Protection Act* (COPPA)[426]. Depuis 1999, enfin, la Commission fédérale du commerce partage, avec d'autres agences, le pouvoir, sous le *Gramm-Leach-Bliley Act* (GLBA)[427], d'établir les « standards appropriés pour les institutions financières soumises à [sa] juridiction », afin « d'assurer la sécurité et la confidentialité des informations et dossiers des consommateurs » et de prémunir « contre les accès non autorisés »[428].

75. Mais déjà en 1995, la FTC était invitée par le Congrès à s'intéresser plus largement à la vie privée, ce qui la conduisit à mener des études sur les politiques de confidentialité des entreprises et à promouvoir, à force reprises, des modèles d'autorégulation[429] qui étaient perçus, à l'époque, comme un moyen terme acceptable dans une perspective de développements des activités numériques. Constatant, toutefois, dans son troisième rapport de 2000, que le modèle de l'autorégulation avait fait long feu, la FTC recommandait au Congrès d'adopter une loi imposant, de manière générale, aux entreprises, le respect des « *fair information practices* »[430], en particulier le *notice and choice model*[431]. Confrontée à l'inertie du législateur, la Commission fédérale du Commerce a donc fait le choix, en plus de ses démarches pédagogiques auprès du public et incitatives auprès des entreprises, de développer le pouvoir contrôle qu'elle avait progressivement mis en œuvre sur le fondement de la section 5[432] du FTCA[433]. Le pouvoir de la FTC n'est en l'occurrence qu'indirect, puisque son intervention est conditionnée par la démonstration d'une pratique « trompeuse » ou « déloyale ». Elle ne dispose d'aucun moyen, comme le permet par exemple le *Fair Credit Reporting Act*, d'agir directement au constat d'une violation du texte[434]. Mais la force de la commission a été de développer deux modèles de contrôle. Le premier est le modèle *notice-and-choice* mis au jour pour appréhender les pratiques trompeuses ; le second est le modèle *harm-based*, utilisé pour les pratiques déloyales.

76. Pour en comprendre la portée, il importe de noter que la FTC dispose de trois types de pouvoirs : investigation, exécution et poursuite qu'elle peut utiliser pour mettre en œuvre dans le

---

"unfair methods of competition" and thus made it clear that Congress, through 5, charged the FTC with protecting consumers as well as competitors ».

425 15 U.S.C. § 1681.

426 15 U.S.C. § 6501-6506.- V. sur ce point les exemples mentionnés supra, n° 62.

427 15 U.S.C. § 6801-6809.

428 Le GLBA, tout comme le COPPA, repose sur un modèle de notice and choice ; sur lequel, v. supra, n° 79.

429 FTC, Privacy Online : Fair Information Practices in the Electronic Markeplace.- A Report to Congress, FTC, May 2000 (http://www.ftc.gov/reports/privacy2000/privacy2000.pdf) ; v. aussi les réf. données par D.J. Solove, W. Hartzog, art. préc., spéc. n° 46, p. 10.

430 V. supra, n° 16 & infra, n° 84.

431 FTC, Privacy Online : Fair Information Practices in the Electronic Markeplace, op. cit., p. 36-37.

432 15 U.S.C. § 45 (2006).

433 V. ainsi GeoCities, FTC Dkt. No. C-3849 (Feb. 12, 1999) ; Liberty Financial Companies, Inc., FTC Dkt. No. C-3891 (Aug. 12, 1999) ; FTC v. ReverseAuction.com, Inc., No. 00-0032 (D.D.C. Jan. 6, 2000).

434 V. les remarques de D.J. Solove, W. Hartzog, art. préc., note (74), p. 15.

cadre de sa mission de protection des consommateurs. La Commission peut, en particulier, « poursuivre toute investigation nécessaire à sa mission dans n'importe quelle partie des États-Unis » et « réunir et compiler des informations et enquêter à tout moment sur l'organisation, les affaires, la conduite, les pratiques et la direction de toute personne, entreprise ou société exerçant des activités commerciales ou dont les affaires affectent le commerce »[435]. À partir des informations qu'elle recueille par ce biais, mais surtout (compte tenu de la faiblesse de ses moyens) par voie de plaintes et dénonciations et grâce aussi à la presse, la FTC peut décider d'introduire une « *enforcement action* » (mesure d'exécution) si elle a des « raisons de croire » que la loi est violée ou a été violée[436]. Et si, au terme de ses investigations, il lui apparaît que des mesures correctrices sont à adopter, elle peut alors délivrer un « *complaint et order* », c'est-à-dire un acte de mise en accusation portant indication de la nature de l'acte illégal allégué et du remède proposé[437]. Il revient alors à la personne mise en cause de choisir soit la voie du règlement amiable, soit celle du règlement judiciaire.

77. En pratique, la grande majorité des procédures initiées se terminent par des « *consent orders* »[438], c'est-à-dire des « ordonnances sur consentement » qui donnent en quelque sorte force exécutoire au règlement amiable obtenu[439]. Quoique ces ordonnances puissent être demandées par la partie poursuivie (lorsque le « temps, la nature de la procédure et l'intérêt du public le permettent »)[440], elles sont presque toujours initiées par la Commission qui décrit, dans l'un de ses documents rendus publics, le déroulement de la procédure : « Si le défendeur choisit de régler amiablement les accusations <*elects to settle the charges*>, il doit alors signer un acte d'engagement <*consent agreement*> (sans reconnaître sa responsabilité), consentir à une ordonnance définitive et renoncer à ses droits à un recours. Si la Commission accepte l'acte d'engagement, elle verse alors l'ordonnance au dossier pendant trente jours aux fins de consultation publique (ou pour toute autre période que la Commission peut préciser) avant de déterminer si elle doit rendre l'ordonnance définitive »[441]. Pour les entreprises, une telle procédure présente de nombreux avantages : échappant à l'obligation de reconnaître sa faute (ce dont elle pourrait tirer mauvaise presse), l'entreprise est surtout assurée d'une sanction bien plus faible que celle qui pourrait lui être infligée à l'issue d'une procédure coûteuse et très incertaine.

---

435 FTC Act Sec. 6(a), 15 U.S.C. Sec. 46(a)). cf. FTC, Office of the General Counsel, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, FTC (July 2008) http://www.ftc.gov/ogc/brfovrvw.shtm.

436 FTC, Office of the General Counsel, A Brief Overview..., op. cit.

437 16 C.F.R., § 2.31, 2.32.

438 16 C.F.R. § 2.31 à 2.34.

439 Sur les 153 complaints qu'ils ont recensés, Solove et Hartzog n'ont relevé qu'une seule action terminée par une décision d'une juridiction : FTC v. Accusearch, 570 F.3d 1187 (10th Cir. 2009).- Cf. D.J. Solove, W. Hartzog, « The FTC and the New Common Law of Privacy », art. préc. p. 14, p. 18, qui indiquent qu'une affaire est également pendante devant une juridiction fédérale : FTC v. Wyndham Worldwide Corp. et al., No. 12-1365 (sur laquelle, J. Sartain, « Analyzing FTC v. Wyndham », International Association of Privacy Professionals (oct. 5 2012), https://www.privacyassociation.org/publications/2012_10_11_analyzing_ftc_vs._wyndham.

440 16 C.F.R., § 2.31.

441 Fed. Trade Comm'n, Office of the General Counsel, A Brief Overview ..., op. cit.

78. Ce n'est évidemment pas à dire que la procédure reste sans conséquence pour l'entreprise. Tout à l'inverse. En premier lieu, toute entreprise violant une ordonnance s'expose à une amende civile pouvant s'élever à $16 000 par violation[442]. En plus de cette amende, la cour de district saisie peut délivrer des « injonctions impératives » (« *mandatory injunctions* »), ainsi que toute mesure équitable[443]. Il faut croire que les accords négociés sont respectés par les entreprises, puisque l'amende civile n'a été prononcée qu'une seule fois dans l'affaire *United States v. Google*[444]. Ils ne sont pourtant pas de ceux qu'une entreprise commerciale, qui retire de grands profits de l'exploitation des données personnelles, est spontanément encline à respecter. Et c'est ce qu'il convient de relever en second lieu : la gamme des mesures pouvant être prononcées par la FTC est remarquablement étendue, sans compter que la FTC peut encore moduler la durée de ces mesures (20 ans, par exemple, pour les obligations de rapport et d'audit, à perpétuité pour d'autres obligations – ce qui a pour effet de lier successeurs et ayant droits), en fonction des objectifs particuliers poursuivis et de la gravité des atteintes constatées[445]. Au-delà de l'interdiction, pour l'avenir, des activités illégales à l'origine de l'intervention de la FTC – qui forme le cœur de toute ordonnance de la FTC[446] –, ou bien encore des amendes et sanctions monétaires diverses[447], l'ordonnance peut comprendre la notification aux consommateurs des violations et de mesures de réparation[448], l'obligation de modifier les politiques en matière de vie privée et d'assurer une meilleure information des utilisateurs[449], la mise en place d'une programme détaillé de sécurité, de vie privée et d'intégrité des données[450], l'évaluation régulière réalisée par un

---

442 Commission Approves Federal Register Notice Adjusting Civil Penalty Amounts, FTC (Dec. 23, 2008).

443 En revanche, aucun mécanisme de recours (« cause of action ») n'a été créé au profit des consommateurs qui ne peuvent que s'en remettre à la FTC.

444 United States v. Google, Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment, No. CV 12-04177 SI.

445 Cf. United States v. Godwin, Consent Decree and Order for Civil Penalties, Injunction and Other Relief, FTC File No. 112303 (N.D. Ga. 2011) ; v. aussi, D.J. Solove, W. Hartzog, op. cit., p. 20.

446 D.J. Solove, W. Hartzog, op. cit., p. 20.

447 Les sanctions s'échelonnent entre $2 000 (FTC v. Guzzetta, Stipulated Final Judgment and Order for Permanent Injunction and Monetary Relief, FTC File No. 012 3066 (E.D.N.Y) ; FTC v. Garrett, Stipulated Final Judgment and Order for Permanent Injunction and Monetary Relief, FTC File No. 012 3067 (S.D. Tex. 2002)) et $35 millions (FTC v. Lifelock, Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief As To Defendants LifeLock and Davis, FTC File No. 072 3069 (D. Ariz. 2010). Dans l'affaire United States v. Godwin (Consent Decree and Order for Civil Penalties, Injunction and Other Relief, FTC File No. 1123033 (N.D. Ga. 2011)), l'amende, initialement fixée à $100 000, a été ramenée à $1 000.- Assez souvent, les entreprises s'engagent également à la remise des profits illégaux ou supportent une mesure de gel des biens.

448 La réparation peut être en nature. Il en est ainsi lorsque la FTC exige d'une entreprise qu'elle mette au point une mise à jour destinée à corriger les failles que présente un logiciel du point de vue de la confidentialité des données (FTC v. Frostwire, LLC, Stipulated Final Order, No. 11-cv-23643 (S.D. Fla. 2011)). Certaines entreprises peuvent également s'engager à rembourser aux consommateurs les produits associés à des pratiques trompeuses (In re US Search, Decision and Order, FTC File No. 1023131). Dans l'affaire ChoicePoint, enfin, la FTC a obtenu de l'entreprise le paiement de $5 millions destinés à réparer les préjudices subis par les consommateurs (United States v. Choicepoint, Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, FTC File No. 052-3069 (N.D. Ga. 2006)).

449 United States v. Sony BGM, Consent Decree, No. 08 Civ. 10730). Si l'entreprise n'a aucune politique en matière de confidentialité, la FTC peut requérir de l'entreprise qu'elle en crée une, le cas échéant sous son autorité.

450 V. D.J. Solove, W. Hartzog, op. cit., p. 22). Dans l'affaire dite « Google Buzz », par exemple (In re Google, Decision and Order, FTC File No. 102 3136), l'ordonnance sur consentement prévoyait la mise en œuvre d'un

professionnel indépendant[451] ou l'obligation de conservation de certains fichiers à laquelle peut être associée une obligation rapport[452]. Mais la mesure principale au regard du droit à l'oubli reste l'exigence d'effacement des informations illégalement collectées ou l'interdiction d'utilisation de ces informations. Cette obligation, presque toujours incluse dans les accords venant constater une violation du COPPA, est aujourd'hui assez souvent imposée au-delà, lorsqu'il est établi que des informations personnelles ont été obtenues au moyen de pratiques trompeuses. Dans l'affaire *In re Aspen Way*[453], par exemple, l'ordonnance faisait obligation au défendeur d'« [e]ffacer ou détruire toutes les données utilisateurs recueillies précédemment en utilisant une technologie de contrôle ou de suivi de localisation géophysique ». C'est ce dernier aspect qui montre peut-être le mieux que la FTC est aujourd'hui devenue la principale gardienne de la vie privée informationnelle.

B- La FTC, gardienne de la vie privée informationnelle

79. Chargée de sanctionner les actes et pratiques trompeurs et déloyaux, la FTC utilise, ainsi qu'on l'a déjà indiqué, deux modèles de contrôle. Le premier est le *notice-and-choice model*, développé dans le domaine de tromperie. Son point de départ constitue une déclaration de politique qui a pris la forme d'un courrier adressé par celui qui était alors le directeur de la FTC, James C. Miller, à un membre du Congrès, John D. Dingell, qui était quant à lui directeur de la *Commission on Energy and Commerce*, à la Chambre des Représentants. C'est dans cette lettre, datant du 14 octobre 1983[454], qui n'a pas été adoptée à l'unanimité des membres de la Commission, que se trouvent pour la première fois exposés les éléments essentiels pris en compte par la FTC pour déterminer si une pratique est ou non trompeuse. On en trouve également un résumé dans l'affaire *Cliffdale Associates*, qui date de l'année suivante. Il ressort de ces documents que la Commission retient la tromperie s'« il y a une *representation*, une omission ou une pratique » qui est « susceptible de tromper le consommateur agissant raisonnablement dans les circonstances », étant ajouté que la « *representation* »[455], l'omission ou la pratique doit être « *material* »[456]. L'acte ou la

---

« programme détaillé de vie privée qui [est] raisonnablement conçu pour : (1) régler les risques de sécurité liés au développement et à la gestion des produits et services pour les consommateurs, nouveaux ou existants ; et (2) protéger la vie privée et la confidentialité des informations visées ». Dans le détail, cela implique l'identification des risques, la formation des employés, la nomination d'un responsable chargé de la coordination du programme et la mise en place d'un processus d'évaluation régulier du programme. Un programme comparable a été imposé à Facebook, dans une autre affaire (In re of Facebook, Inc., Agreement Containing Consent Order, File No. 092 3184 (2011)).

451 Les entreprises poursuivies pour des pratiques déloyales ou trompeuses en matière de sécurité des données s'engagent souvent à une évaluation bisannuelle réalisée par un professionnel indépendant qui s'assure du respect de l'ordonnance.

452 Presque toutes les entreprises qui négocient avec la FTC s'engagent à des enregistrements de données afin de faciliter l'activité de suivi de l'exécution des ordonnances. Dans de très nombreuses affaires, les entreprises s'engagent également à produire régulièrement des rapports (D.J. Solove, W. Hartzog, op. cit., p. 23).

453 In re Aspen Way, Agreement Containing Consent Order, FTC File No. 112 3151.

454 Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to Hon. John D. Dingell, Chairman, Comm. on Energy and Commerce, U.S. House of Representatives (Oct. 14, 1983) :
http:// www.ftc.gov/oia/assistance/consumerprotection/advertising/policy_deception.pdf (v. aussi en appendice in Cliffdale Associates, Inc., 103 F.T.C. 110 (1984)).

455 Sur la notion de representation, v. supra, note n° (325).

456 Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984).

pratique doit, tout d'abord, être « *susceptible de tromper* ». En d'autres termes, il n'est pas nécessaire que le consommateur ait été effectivement trompé, et il suffit de démontrer que la *representation,* l'omission ou la pratique était de nature à tromper[457] un consommateur raisonnable[458]. Quant à la *materiality*, il s'agit de déterminer, comme dans le cadre de l'*estoppel by representation* par exemple, l'importance de l'information pour le consommateur, avec cette question en particulier : cette information a-t-elle ou non affecté son choix[459] ? La FTC a généralement soin d'analyser un faisceau d'indices tirés du document en son entier, de la juxtaposition des phrases dans le document, de la nature de la déclaration ou de la transaction[460]. Sous ce regard, est souvent *material* la tromperie qui porte sur les caractéristiques principales du produit, comme sa sécurité, son coût ainsi que adéquation avec la finalité pour laquelle il est vendu[461]. En revanche, il n'est pas nécessaire de montrer que le consommateur n'aurait pas acheté le produit sans la tromperie[462]. Enfin, et plus généralement, il n'est pas nécessaire d'établir que le défendeur avait l'intention de frauder ou de tromper[463].

80. Le second modèle est appelé *harm-based model*, développé, quant à lui, dans le domaine de la déloyauté (*unfairness*). Depuis deux arrêts de la Cour Suprême, le premier *FTC v. Raladam Co.*, de 1931[464], surtout le second, *FTC v. Sperry & Hutchinson Co.*, de 1972[465], il est acquis que la FTC peut sanctionner les comportements déloyaux, sans avoir à établir la violation d'une règle particulière en matière de concurrence. Tirant argument de ce que l'objectif du *Federal Trade Commission Act* (FTCA) est de prévenir les préjudices causés aux consommateurs, la FTC a ainsi décidé que le constat du préjudice pouvait à lui seul supporter la démonstration de ce qu'une pratique est déloyale[466]. La FTC utilise un triple filtre : (1) la présence d'un préjudice substantiel[467]

---

457 Cliffdale..., op. cit. p. 165.

458 Le standard est en effet constitué du consommateur raisonnable. Dans sa lettre précitée, de 1983, la FTC notait : « Certaines personnes, par ignorance ou incompréhension, peuvent être trompées y compris par une déclaration scrupuleusement honnête. Peut-être quelques esprits égarés croient, par exemple, que toutes les viennoiseries [Danish pastry dans le texte] sont faites à Vienne [Danemark dans le texte]. Y a-t-il une tromperie susceptible de donner lieu à réparation dans le fait d'afficher "viennoiserie" [Danish pastry] dans notre pays ? Évidemment non. Une representation ne devient pas "fausse et trompeuse" simplement parce qu'elle serait mal comprise de manière non raisonnable par une fraction insignifiante et non représentative de la classe de personnes à laquelle la representation est adressée ». Cependant, la FTC analyse des segments de marché de consommateurs spécifiques si l'acte ou la pratique cible un groupe particulier (Ideal Toy Corp., 64 F.T.C. 297, 310 (1964)). D'autres informations sont également prises en compte : quel est le degré de clarté de la representation ? L'information est-elle visible et, le cas échéant, dans quelle mesure ? Quelle est l'importance de l'information omise ? N'existait-il pas d'autres sources susceptibles de suppléer au défaut d'information ? Quelle est la familiarité du public avec le produit ou le service ? (Lettre de la FTC, op. cit., p. 6).

459 Cliffdale..., op. cit., p. 165-166 ; Am. Home Prods. Corp., 98 F.T.C. 136; Ford Motor Co., 84 F.T.C. 729, 735 (1974).

460 Cliffdale..., op. cit. p. 166 ; Bristol-Myers Co., 102 F.T.C. 21 (1983).

461 Int'l Harvester Co., 104 F.T.C. 949, 1057 (1984).

462 Leonard F. Porter, Inc., 88 F.T.C. 546, 628 (1976); Travel King, Inc., 86 F.T.C. 715, 774 (1975).

463 FTC v. World Travel Vacation Brokers, Inc., 861 F.2d 1020, 1029 (7th Cir. 1988).

464 FTC v. Raladam Co., 283 U.S. 643, 648 (1931).

465 Federal Trade Commission v. Sperry & Hutchinson Trading Stamp Co., 405 U.S. 233 (1972).

466 FTC, Policy Statement on Unfairness, FTC, Washington DC, (December 17, 1980), Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984) : « Unjustified consumer injury is the primary focus of the FTC Act, and the most important of the three S&H criteria. By itself it can be sufficient to warrant a finding of unfairness. The

(2) qui n'est pas contrebalancé par un bénéfice retiré par le consommateur ou par le droit de la concurrence (libre concurrence)[468] ; (3) le préjudice est de ceux que les consommateurs n'auraient pu raisonnablement éviter[469]. En pratique, et pour renforcer son analyse tripartite, la FTC s'appuie également sur la violation d'une règle d'intérêt public (« *violation of public policy* »). Elle recherche si l'acte ou la pratique viole une règle de cette nature établie par la loi (« *statute law* »), par le *common law*, les bonnes pratiques de l'industrie (codes, chartes, etc.). Et du constat de la violation de l'une de ces règles, en présence, bien entendu, d'un préjudice, la FTC peut alors inférer la conduite immorale (« *unethical* ») ou malhonnête (« *unscrupulous* ») qui caractérise la déloyauté.

81. C'est sur l'un ou l'autre de ces fondements que la FTC a pu développer une ligne jurisprudentielle particulièrement énergique qui est aujourd'hui suivie avec le plus grand intérêt par les responsables des traitements de données au sein des entreprises privées. Sur le terrain de la tromperie, qui représente la plus grande partie de sa jurisprudence, la FTC n'a généralement

---

Commission's ability to rely on an independent criterion of consumer injury is consistent with the intent of the statute, which was to "[make] the consumer who may be injured by an unfair trade practice of equal concern before the law with the merchant injured by the unfair methods of a dishonest competitor" »).

467 Le préjudice ne peut être simplement véniel ou potentiel. Il doit être d'ordre monétaire ou toucher à la santé ou à la sécurité des personnes. Un préjudice simplement psychologique n'est en revanche pas suffisant. Dans l'affaire FTC v. Accusearch (570 F.3d 1187, 1193-94 (10th Cir. 2009)), une juridiction du 10e circuit a précisé, par un obiter dictum, que le fait de poster en ligne les noms et numéros téléphoniques des abonnés pouvait causer aux consommateurs un préjudice émotionnel, en raison du risque d'être harcelé, mais aussi préjudice économique, en raison des coûts impliqués par un changement de fournisseur d'accès. Il s'agissait, selon la juridiction, d'un préjudice substantiel.

468 La FTC examine les coûts et bénéfices respectifs et ne retient que la pratique qui est préjudiciable « dans ses effets nets » (« The Commission is aware of these tradeoffs and will not find that a practice unfairly injures consumers unless it is injurious in its net effects », FTC, Policy Statement on Unfairness, op. cit.). La Commission tient surtout compte des coûts que représente l'intervention de la FTC pour la société (l'économie) dans son ensemble : frais bureaucratique, impact des charges réglementaires sur la circulation de l'information, réduction des incitations à l'innovation, etc. (« The Commission also takes account of the various costs that a remedy would entail. These include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters », ibid.).

469 Selon le postulat libéral qui soutient la doctrine de la FTC, le marché alloue normalement les ressources de manière optimale. Du point de vue du consommateur, cela signifie que l'Homo œconomicus qui compose le marché étudie toujours les alternatives disponibles, porte son choix sur la branche qui lui est la plus profitable et rejette celle qui est économiquement inadéquate. Le consommateur raisonnable (au sens économique) évite donc un certain nombre de choix et c'est à la lueur de ce consommateur-standard que doit être évalué le préjudice. Il arrive toutefois que la complexité de certaines opérations conduise le consommateur à faire de mauvais choix. Des mesures correctrices peuvent alors s'avérer nécessaires. C'est en cette hypothèse qu'on peut dire que le préjudice ne pouvait être raisonnablement évité par le consommateur (« Normally we expect the marketplace to be self-correcting, and we rely on consumer choice – the ability of individual consumers to make their own private purchasing decisions without regulatory intervention – to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking », FTC, Policy Statement on Unfairness, op. cit.).

aucun mal à sanctionner les entreprises qui méconnaissent les engagements clairs et explicites qu'elles ont pris en matière de confidentialité. Ainsi en est-il de l'entreprise qui viole l'engagement expresse à maintenir la confidentialité des données ou à s'abstenir de les divulguer à des tiers[470] ; ainsi encore de l'entité commerciale qui collecte des données au-delà des limites qu'elle s'était elle-même fixées dans sa politique de confidentialité[471]. La sanction est la même pour la compagnie qui s'était engagée à offrir une protection adéquate des données personnelles, ce qui, à l'examen, s'avère parfaitement inexact[472]. Enfin, entre dans cette catégorie d'affaires qui ne présentent généralement guère de difficultés d'analyse pour la FTC, celles dans lesquelles l'entreprise, qui s'était engagée à garantir l'anonymat des données, viole manifestement la promesse qu'elle avait faite[473]. Au-delà de ces engagements pris en matière de confidentialité, la Commission s'attache également à sanctionner les manœuvres trompeuses destinées à provoquer la divulgation de certains informations, comme c'était par exemple le cas dans l'affaire *In re ReverseAuction.com, Inc*, où l'entreprise poursuivie avec obtenu d'Ebay – son concurrent – des informations personnelles qu'elle utilisait ensuite pour rediriger les utilisateurs de son concurrent vers son propre site Internet[474]. Dans le prolongement, est grossièrement trompeuse la pratique commerciale destinée à conduire le consommateur à télécharger des logiciels espions[475]. Si l'entreprise peut mettre en place des dispositifs de surveillance (qui collectent des données), encore faut-il qu'elle en informe les utilisateurs ; et une information incomplète (certains dispositifs de surveillance étant laissés dans l'ombre, par exemple) suffit à caractériser la tromperie[476].

82. Avec peut-être un peu moins d'éclat, la FTC s'est également attachée à sanctionner les déloyautés sur le fondement du *harm-based model*. D'après les résultats de l'étude menée par D. Solove et W. Hartzog[477], la FTC sanctionne cinq types de comportements sur le fondement de la déloyauté. Il s'agit tout d'abord des changements rétroactifs dans les règles en matière de confidentialité. Dans l'affaire *In re Gateway Learning Corp.* (2004)[478], l'entreprise poursuivie avait

---

470 In re Eli Lilly, Complaint, File No. 012 3214 (In the Matter of Eli Lilly and Company, a corporation, Decision and Order, Docket No. C-4047). V. aussi, c cas particulier d'engagement violé à l'occasion d'une vente de données au cours d'une procédure de liquidation judiciaire avec cessions d'actifs : FTC v. Toysmart, First Amended Complaint for Permanent Injunction and Other Equitable Relief, File No. X000075.

471 In re HTC America Inc., FTC File No. 122 3049 ; In re Microsoft Corporation, File No. 012 3240.

472 In re Microsoft Corporation, File No. 012 3240 (précité) ; In the Matter Genica, File No. 082 3113.

473 In re Compete, File No. 102 3155.

474 FTC v. Reverseauction.com, Inc., FTC File. No. 002-3046 (D.D.C. Jan. 6, 2000). Avant d'obtenir ces informations, l'entreprise ReverseAuction s'était abonnée à eBay et avait souscrit à l'accord relatif à la protection de la vie privée des utilisateurs de cette société, faisant interdiction à ces mêmes utilisateurs de recueillir et d'utiliser des données personnelles à des fins non autorisées, notamment l'envoi de messages électroniques commerciaux non sollicités. Pour la FTC, ReverseAuction avait donc menti en déclarant qu'elle s'engageait à respecter l'accord.

475 In re DesignerWare, LLC, FTC File No. 112 3151 ; In re B. Stamper, Complaint, File No. 112 3151 ; In re C.A.L.M. Ventures, Inc., also doing business as Premier Rental Purchase, Complaint, File No. 112 3151 ; In re J.A.G. Rents, LLC, also doing business as ColorTyme, Complaint, File No. 112 3151 ; In re Red Zone Investment Group, Inc., also doing business as ColorTyme, File No. 112 3151 ; In re Watershed Development Corp., also doing business as Watershed and Aaron's Sales & Lease Ownership, Complaint, File No. 112 3151.

476 In re Epic Marketplace, Inc., and Epic Media Group, LLC, Complaint, File No. 112 3182 ; Sears Holdings Management Corporation, a corporation, Complaint, File No. 082 3099.

477 D.J. Solove, W. Hartzog, « The FTC and the New Common Law of Privacy », op. cit.

478 Gateway Learning Corp. FTC, File No. 042-3047 ; v. aussi, In re Facebook, Complaint, File No. 092 3184.

modifié ses règles de vie privée de manière à autoriser le transfert des données à des tiers, ce à quoi s'opposaient expressément la précédente politique de confidentialité. L'entreprise n'avait pas informé les consommateurs de ces changements, en dépit du fait qu'elle avait expressément indiqué à ses utilisateurs que « [s]i à une date ultérieure nos pratiques d'usage des informations venaient à connaître un changement important qui affecte vos données personnelles, nous vous notifierions tous les changements pertinents ». Il s'agit ensuite des pratiques consistant à installer des logiciels espions, manœuvres qui, lorsqu'elles n'avaient fait l'objet d'aucun engagement de la part de l'entreprise[479], tombent sous le coup de la déloyauté[480]. La FTC peut encore sanctionner l'utilisation inappropriée des données, qui vient généralement s'ajouter à un grief de collecte illicite d'informations[481], ou bien poursuivre en raison de la déloyauté de la conception du site Internet ou des règles de paramétrage par défaut. Enfin, la Commission peut être amenée à intervenir en raison de pratiques déloyales[482] en matière de sécurité[483].

83. Ce sont surtout les sanctions, que la FTC n'hésite pas à prononcer contre les entreprises poursuivies dans le cadre de la section 5, qui montrent tout à la fois que le droit américain perçoit l'intérêt d'une plus grande autonomie dans la sphère informationnelle et dispose des moyens d'offrir aux utilisateurs une plus grande maîtrise de leurs données personnelles. Parmi ces moyens, il faut bien entendu évoquer l'effacement des données, mesure que la Commission réserve apparemment aux violations les plus graves, de manière anéantir l'atteinte portée à la vie privée informationnelle avant la mise en vigueur de règles plus protectrices des données de la part de l'entité condamnée. Les *misrepresentations* portant sur les garanties d'anonymat[484] et de non-divulgation des données peuvent ainsi conduire la FTC à exiger la suppression de toutes les données collectées au moyen de la tromperie. Dans l'affaire *Compete, Inc.*, mettant justement en jeu une tromperie en matière d'anonymat des données, l'ordonnance sur consentement indiquait ainsi que « Compete, Inc., ses successeurs et ayants droit, dans les quatorze (14) jours après la date de signification de cette ordonnance, effaceront ou détruiront les informations collectées, en leur possession ou leur contrôle, recueillies avant le 1er février 2010, sauf indication contraire de l'un des membres de la Commission »[485]. La mesure est également systématiquement ordonnée lorsque la FTC a constaté le recours à des dispositifs d'espionnage,

---

479 V. supra, n° 81, pour les hypothèses de tromperie.

480 La FTC regarde si un préjudice a été causé au consommateur : In re Aspen Way, Complaint, File No. 112 3151 ; In re Sony BMG Music Entertainment, a general partnership, complaint, File No. 062-3019.

481 Tel était le cas dans l'affaire In re Aspen Way, précitée.

482 In re BJ's Wholesale Club, Inc., File No. 042 3160.

483 Lorsque l'entreprise a pris l'engagement d'assurer la sécurité des données, la FTC retient la misrepresentation. Cf. In the Matter Compete, Complaint, File No. 102 3155, précité ; FTC v. Sandra L. Rennert, Philip Rennert, Lyle Mortensen, International Outsourcing Group, Inc., Focus Medical Group, Inc., Trimline, Inc., Affordable Accents, Inc., World Wide RX, Inc., World Wide Medicine, Inc., PSRenn, Inc., and Doctors A.S.A.P., Inc., complaint No. 992 3245, File No. 992 3245 ; In re Eli Lilly, Complaint, File No. 012 3214, précité.

484 En cette hypothèse, l'effacement n'est pas exigé : v. par ex. In the Matter of Eli Lilly and Company, a corporation, Decision and Order, Docket No. C-4047. V., toutefois, dans l'affaire FTC v. Toysmart, précitée, spéc. § II.

485 In the Matter of Compete, Decision and order, Docket No. C-4384, § VII.

qu'elle se place du reste sur le terrain de la tromperie[486] ou sur celui de la déloyauté[487]. Lorsque les violations de la section sont à des changements rétroactifs de politiques de confidentialité[488] ou la conception déloyale des sites ou des règles de paramétrages en matière de protection des données[489], la FTC n'ordonne semble-t-il pas l'effacement des données. Mais les sanctions qu'elles imposent accroissent incontestablement la vie privée informationnelle des utilisateurs en redonnant toute sa place au consentement de la personne. En imposant un mécanisme d'*opt-in* dans le cadre d'un changement rétroactif de règles en matière de confidentialité ou de paramétrages par défaut déloyaux, la FTC autorise de manière effective les consommateurs à échapper à la collecte, au traitement et à la divulgation de certaines données, ce qui est un net progrès. Il ne faut toutefois pas outrer la portée du mécanisme qui ne dit évidemment rien du retrait possible du consentement et éloigne alors de la question du droit à l'oubli que seule garantit la sanction de l'effacement[490]. Sans compter que bon nombre de secteurs importants échappent à la compétence de la FTC[491].

Conclusion

---

486 FTC v. Reverseauction.com, Inc., FTC File. No. 002-3046 (D.D.C. Jan. 6, 2000) ; In the Matter of DesignerWare, Docket No. C-4390, Consent and Order ; In re B. Stamper, Docket No. C-4393, Decision and Order, § V ; In the Matter of C.A.L.M. Ventures, Inc., Docket No. C-4394, Decision and Order § V ; In the Matter of J.A.G. Rents, LLC, Docket No. 4395, Decision and Order, § V ; In the Matter of Red Zone Investment Group, Inc., Docket No. C-4396, Decision and Order, § V ; In the Matter of Watershed Development Corp., Docket No. C-4398, § V. C'est la formule suivante qui est généralement employée : « V. PROTECTION OF DATA IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, and its officers, agents, servants, employees, and all persons or entities in active concert or participation with it who receive actual notice of this order, by personal service or otherwise, shall :— A. Delete or destroy all user data previously gathered using any monitoring or geophysical location tracking technology that does not comply with Parts I, II, and III of this Order, unless such action is otherwise prohibited by court order or other legal obligation [...] ».- V. encore : In the Matter of Epic Marketplace, Inc., Docket No. C.-4389, Decision and Order, § III ; In the Matter of Sears Holdings Management Corporation, Docket No. C-4264, Decision and Order, § III.

487 In re Aspen Way, Docket No. C-4392, Decision and Order, § V.

488 In the Matter of Gateway Learning Corp., Docket No. C-4120, Decision and Order, spéc. § II ; In re Facebook, Docket No. C-4365, Decision and Order, spéc. § II.

489 FTC v. Frostwire, LLC, No. 11-cv-23643 Stipulated Final Order for Permanent Injunction, Case No. 11-23643-CV-GR.

490 V. toutefois les décisions prononcées dans le domaine des failles de sécurité : Stipulated Final Order for Permanent Injuction as to Lyle Mortensen, Civil Action No. CV-S-00-0861-JBR, spéc. § IV : "IT IS FURTHER ORDERED that defendant Mortensen [...] shall : [...] C. Provide reasonable means by which a consumer may modify inaccurate personal information or delete personal information, concerning him or her" ; Stipulated Final Order for Permanent Injunction as to Sandra L. and Philip Rennert and Corporate Defendants, Civil Action No. CV-S-00-0861-JBR, spéc. § IV, même mesure.

491 15 USC § 45(a)(2). Sont concernés les établissements financiers, les sociétés de télécommunications et les entreprises publiques de transport inter-États, les transporteurs aériens, les conditionneurs et les conditionneurs et les exploitants de parcs à bestiaux. Cf. Décision de la Commission du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (2000/520/CE), JOCE 25.8.2000, L 215/7.

84. En 1997, l'administration Clinton pressait déjà les entreprises américaines à réformer leurs pratiques en matière de traitement des données personnelles, à peine d'adoption d'un cadre législatif[492]. Quinze ans plus tard, le bilan n'est pas difficile à dresser. Non seulement le document n'a pas eu l'effet incitatif escompté, mais on peut même dire que ces dernières décennies ont montré que les entreprises pouvaient également compter sur le soutien des juridictions – au risque d'entamer la confiance dans le commerce électronique. La Maison Blanche n'en est que trop consciente qui a récemment publié, sous la responsabilité du *Department of Commerce*, un nouveau rapport intitulé : *Consumer Data Privacy in a Networked World : A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*[493]. L'ambition du texte est remarquable, puisqu'il s'agit rien moins que de promouvoir un *Consumer Privacy Bill of Rights* qui intègre une version dite « compréhensive et globale » des *Fair Information Practice Principles*[494]. Le champ d'application de la Charte[495], de même que son contenu, témoignent d'une volonté réelle de mieux garantir la vie privée des consommateurs. Sept principes viennent ainsi réactualiser les *Fair Information Practices* : (1) contrôle individuel ; (2) transparence ; (3) respect du contexte ; (4) sécurité ; (5) accès et exactitude ; (6) minimisation dans le récolement des données ; (7) *accountability*[496]. Il est surtout notable d'assister au déploiement d'une forme de droit à l'oubli. Au titre du principe de transparence, par exemple, il est indiqué que les entreprises doivent fournir une description claire des données personnelles qu'elles collectent, des besoins qu'elles entendent satisfaire, de l'usage qu'elles leur réserve, et du moment où ces données seront effacées ou désidentifiées[497]. Enfin, et surtout, le principe d'accès et d'exactitude devrait conduire à ce que les entreprises fournissent aux consommateur un accès raisonnable aux données personnelles qu'elles recueillent ou conservent, ainsi que des moyens appropriés pour corriger les données inexactes ou demander leur effacement ou leur usage limité[498]. Ces propositions ont d'autant plus de résonance qu'elles s'inscrivent dans un mouvement plus global de prise de conscience de l'enjeu de la vie privée informationnelle. Faisant écho à une proposition du représentant (de la Chambre des

---

492 White House, The Framework for Global Electronic Commerce, 1997 (http://clinton4.nara.gov/WH/New/Commerce/).

493 White House, Consumer Data Privacy in a Networked World : A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, February 2012, Washington (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf).- Sur ce texte, v. M. Rotenberg, D. Jacobs, « Updating the Law of Information Privacy : the New Framework of the European Union », 36 HVJLPP 605 (2013), spéc. p. 649 et s.

494 V. supra, n° 16.

495 White House, Consumer Data Privacy in a Networked World, op. cit., p. 10 : « La Charte des Droits en matière de vie privée du consommateur s'applique à toutes les données personnelles, ce qui signifie toute donnée, y compris les agrégations de données, pouvant être liée à un individu en particulier. Les données personnelles pourraient inclure les données qui sont liées à un ordinateur particulier ou un autre appareil. Le Gouvernement soutient toute législation fédérale adoptant les principes de la Charte des Droits en matière de vie privée du consommateur. Même en l'absence de législation, le Gouvernement réunira les parties prenantes dans un processus de création de codes de conduites contrôlés par la FTC, mis en œuvre sur le modèle de ces droits ».

496 Le terme, qui se laisse difficilement traduire par « responsabilité », est défini infra, n° 87.

497 Op. cit., p. 14.

498 Op. cit., p. 19-20.

représentants) Ed Markey[499], l'État de Californie[500] vient d'adopter une nouvelle loi introduisant un nouveau chapitre dans le *State's Business and Professions Code* (BPC) intitulé : « *Privacy Rights for California Minors in the Digital World* »[501]. Cette série de dispositions novatrices, qui entrera en vigueur le 1er janvier 2015, est destinée à renforcer les droits des mineurs sur l'Internet. La future section 22581(a) retiendra toute l'attention du jursite européen puisque le texte énonce : « L'exploitant d'un site Internet, d'un service en ligne, d'une application en ligne ou d'une application mobile destiné à des mineurs ou qui a connaissance de ce qu'un mineur utilise son site Internet, service en ligne, application en ligne ou application mobile doit faire tout ce qui suit : (1) Autoriser le mineur, qui est un utilisateur enregistré du site Internet, service en ligne, application en ligne ou application mobile de l'exploitant, à procéder à la suppression ou, si l'exploitant préfère, à demander et obtenir la suppression du contenu ou de l'information déposée sur le site Internet, service en ligne, application en ligne ou application mobile de l'exploitant ».

85. Faut-il voir dans ces nouveaux textes les jalons de changement de paradigme aux États-Unis ? Rien n'est moins sûr. Si la récente loi ne dit rien de la liberté d'expression, le *Consumer Privacy Bill of Rights* précise bien, à propos de l'effacement possible des données (*principe d'accès et d'exactitude*), que « [l]es entreprises qui détiennent des données personnelles devraient interpréter ce principe de manière compatible avec la liberté d'expression et la liberté de la presse »[502]. La formule, qui pourrait passer pour une simple nuance, mérite d'être lue à la lumière de l'importance culturelle et structurelle reconnue à la liberté d'expression aux États-Unis[503]. Ainsi qu'on l'a vu, la notion d'oubli[504] n'est pas totalement étrangère au droit américain qui a su la reconnaître à travers *le tort of public disclosure* et les principes de minimisation et de finalité des *Fair Information Pratices*[505]. Elle n'a pourtant jamais réussi à triompher face à la liberté de la presse et la

---

499 Il s'agissait d'intégrer au COPPA une forme de droit à l'oubli : « Do Not Track Kids Act », H.R. 1895 (112th Congress, 1st Session, 2011), cité par M.L. Ambrose, J. Ausloos, « The Right to Be Forgotten Across the Pond », Journal of Information Policy 3 (2013), 1-23, spéc. p. 6, p. 13-14.

500 Sans doute l'État américain qui dispose de la législation la plus protectrice en matière de vie privée ; v. supra, n° 17, la Constitution de Californie qui s'applique également dans les rapports horizontaux.

501 BPC, Chapter 22.1, Section 22580, Division 8, September 23, 2013.

502 White House, Consumer Data Privacy in a Networked World..., op. cit., p. 19.

503 R.K. Walker, « The Right to Be Forgotten », 64 Hastings L.J. 257 (2012), spéc. p. 271 ; v. aussi F. Werro, « The Right to Inform v. the Right to be Forgotten : A Transatlantic Clash », in A. Colombi Ciacchi et al. (ed.), Haftungsrecht im dritten Millenium.- Liber Amicorum Gert Brüggemeier, Nomos, Baden Baden, 2009, p. 286 : « The notion that constitutional rights could be balanced against each other and that the freedom to speak and inform could be balanced against a competing constitutional entitlement to the respect of one's private life does not seem to be an option under United States constitutional law ».- Adde, M. Fazlioglu, « Forget me not : the clash of the right to be forgotten and freedom of expression on the Internet », IDPL 2013, p. 1 et s., spéc. p. 7-9.

504 Plus largement à l'échelle de la culture américaine : M.L. Ambrose, J. Ausloos, art. préc., p. 8, qui évoquent le mythe de l'Ouest américain auquel est associée l'idée d'un nouveau départ – le « going West » : partir pour le grand Ouest.

505 V. en ce sens, S.C. Bennett, « The "Right to Be Forgotten" : Reconciling EU and US Perspectives », 30 Berkeley J. Int'l L. 161 (2012), p. 166-167 ; CDT – Center for Democracy & Technology, Comments of the Center for Democracy & Technology to the European Commission in the Matter of Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union, Washington, January 15, 2011 (http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/cdt_en.pdf), p. 10 : « In the context of passive data sharing, the "right to be forgotten" is to some extent already recognized in the U.S.,

liberté du commerce. Comme le disait Whitman dans un article de droit comparé : « La résistance des Américains à l'égard de la vie privée a toujours été fondée sur deux valeurs en particulier : la liberté de la presse et la liberté du commerce » [506]. Comme l'exprime le grand laudateur du libre discours aux États-Unis, Eugene Volokh, « [n]ous avons déjà un Code de "*fair information practices*" et il s'agit du Premier amendement qui empêche généralement le Gouvernement de "contrôle[r la communication] de l'information" (soit par la régulation directe, soit par l'autorisation des actions en responsabilité civile) qu'elle soit "équitable" <*fair*> ou non »[507]. Il faut du reste ajouter, comme l'a bien observé Franz Wero, que la Cour Suprême croit tellement dans « *free marketplace of ideas* » – libre commerce/échange des idées –, qu'elle doute même de sa compétence dans la détermination de ce qui, sous le Premier amendement, est digne de protection et ce qui ne l'est pas (v., par ex., en matière commerciale)[508]. Transposé au domaine du commerce électronique, l'argument tiré du libre commerce prend un tour concret et véritablement économique : les entreprises doivent pouvoir continuer de collecter et traiter des données personnelles pour accroître leur performance sur le marché.

86. Pour sortir de l'impasse plusieurs solutions paraissent pouvoir être proposées. La première, et qui inspire finalement les rapports récents de la FTC et de la Maison Blanche, est de mettre en évidence la perte de confiance des consommateurs qui pourrait résulter d'une sous-protection de la vie privée et dont les conséquences pour l'économie américaine pourraient être désastreuses[509]. En retournant l'argument du libre-échange au profit de la vie privée, on affaiblit évidemment les arguments favorables à une protection constitutionnelle étendue des traitements de données. Même si le redécoupage du périmètre des discours protégés paraît délicat, il n'est plus possible de soutenir, comme le fait Eugene Volokh[510], que les traitements de données commerciales relèvent d'un contrôle renforcé sous le Premier amendement. Il conviendrait ensuite – et c'est la deuxième solution – de bien insister sur l'argument déjà mis en avant, selon

---

although it is discussed in terms of limitations on data retention and use. For example, the U.S. Fair Credit Reporting Act places limits (quite long ones, to be sure) on the use in credit reports of bankruptcies that occurred years ago ».

506 Q. Whitman, « The Two Western Cultures of Privacy : Dignity versus Liberty », op. cit., p. 1197.

507 E. Volokh, « Freedom of Speech and Information Privacy : The Troubling Implications of a Right to Stop People from Speaking About you », op. cit., p. 1051.

508 F. Wero, op. cit., p. 300.

509 FTC, Protecting Consumer Privacy in Era of Rapid Change: Recommendations for Businesses and PolicyMakers, 2012, p. 8, 11, 12 et passim : « In terms of weighing costs and benefits, although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will benefit businesses by building consumer trust in the marketplace ».- White House, Consumer Data Privacy in a Networked World…, op. cit., p. 5, 6 et passim : « Strong privacy protections also are critical to sustaining the trust that nurtures Internet commerce and fuels innovation. Trust means the companies and technical systems on which we depend meet our expectations for privacy, security, and reliability. […] Preserving trust in the Internet economy protects and enhances substantial economic activity ».

510 E. Volokh, art. préc., p. 1094 : « Plusieurs de ces bases de données [bases de données contenant des informations personnelles] – par exemple, des bases de données sur les antécédents de crédit ou sur les antécédents criminels – sont utilisées par des hommes d'affaires afin de déterminer qui, en affaires, est digne de confiance et qui est susceptible de tromper. D'autres bases de données qui contiennent des informations moins incriminantes, telles que les habitudes d'achat de personnes, pourraient mériter une moindre protection. Mais, bien entendu, c'est précisément parce les données stockées dans ces bases sont aussi bien moins embarrassantes que le dommage prétendument causés à ceux qui sont l'objet de ces communications de données est beaucoup moins important ».

lequel le Premier amendement peut également venir renforcer la vie privée. Cela vaudrait évidemment pour la divulgation de faits de nature privée, mais aussi pour toutes les données personnelles, car comme l'ont bien montré Schwartz[511] et tant d'autres auteurs[512], les « lois en matière vie privée ne reviennent pas à imposer aux parties un silence contraire au Premier amendement. Tant qu'elles conservent un point de vue neutre, ces lois sont plutôt un élément nécessaire à la préservation de la libre communication dans notre société démocratique. La lecture que Volokh livre du Premier amendement cherche à faire absolument et définitivement du discours public la sphère de communication prédominante. [...] Pourtant, une société démocratique dépend tout autant de discours publics que d'autres domaines de communication ». On retrouverait ici les exigences de la démocratie délibérative[513] à laquelle la Cour Suprême ne pourra rester longtemps insensible. Enfin, une dernière solution devrait s'attacher à remettre en débat la notion de discours d'intérêt public[514].

87. Les perspectives d'évolution à court terme restant limitées, il faut consacrer le mot final aux données personnelles. Il faut observer, ce que le débat actuel tend à occulter, que le droit à l'oubli n'est qu'une facette[515] de ce qu'on pourrait appeler *le pouvoir de contrôle des données*[516]. Une plus grande transparence, un meilleur respect des principes de minimisation et de finalité, ainsi

---

511 P.M. Schwartz, « Free Speech vs. Information Privacy : Eugene Volokh's First Amendment Jurisprudence », op. cit., p. 1563.

512 Cf., en particulier, R.C. Post, « The Constitutional Concept of Public Disclosure : Outrageous Opinion, Democratic Deliberation, and Hustler Magazine v. Falwell », 103 Harv. L. Rev. 601 (1990), p. 627-646.

513 V. encore P.M. Schwartz, « Privacy and Democracy in Cyberspace », 52 Vand. L. Rev. 1647 (1999) ; S. Simitis, « Reviewing Privacy in an Information Society », 135 U. Pa. L. Rev. 707 (1987).

514 Sans aller jusqu'à réduire au silence les opinions minoritaires – ce qui ouvrirait la voie à la majorité tyrannique et au conformisme – il faut bien reconnaître que certaines informations sont d'un intérêt public mineur. Se référant à l'affaire Diaz, Eugene Volokh a pu soutenir le contraire (Diaz v. Oakland Tribune (188 Cal. Rptr. 762 (Ct. App. 1983)). Diaz, première femme présidente du conseil étudiant d'un collège communautaire, était transsexuelle. Le fait fut dévoilé par le Oakland Tribune. La Court of Appeals reconnut que l'affaire méritait d'être soumise à un jury ; et si un jury jugeait que le transsexualisme de Diaz n'était pas d'actualité (« newsworthy »), elle pourrait obtenir des dommages intérêts. La cour laissa au jury le soin de déterminer ce point, avec quelques instructions intéressantes : « en déterminant si l'article soumis peut faire l'actualité (« is newsworthy ») vous devez considérer [la] valeur sociale du fait publié, la profondeur de l'article, [son] intrusion dans des affaires apparemment privées, et la mesure dans laquelle la demanderesse a volontairement accédé à une position de personne notoire ». Voilà des questions fondamentales qui devraient évidemment guider les juridictions dans la détermination de ce qui est d'intérêt public et ce qui ne l'est pas. Il se trouvera toujours quelqu'un pour soutenir que le transsexualisme était une information déterminante. Mais n'appartient-il pas au juge de dire, par exemple, qu'il n'est aucun lien entre l'information divulguée et l'aptitude de Diaz à exercer ses fonctions ? Peut-on soutenir, comme le fait Volokh, qu'il ne ressortit jamais à la compétence du juge de dire qui est profondément faux ou immoral ? Qu'il revient seulement au « libre commerce des idées » de faire le tri opinions d'importance et opinions sans intérêt ? (« Toutes ces conceptions peuvent être fausses et même immorales. Mais il n'appartient certainement pas à un agent du Gouvernement – juge ou jury – de dicter les critères politiques en matière de choix politiques de citoyens et d'utiliser la force contraignante du droit pour empêcher autrui de les informer de certaines choses qu'ils pourraient juger pertinentes pour faire leur choix », E. Volokh, « Freedom of Speech and Information Privacy : The Troubling Implications of a Right to Stop People from Speaking About you », op. cit., p. 1090).- V. aussi R.G. Larson III, « Forgetting the First Amendment : How Obscurity-Based Privacy and a Right to be Forgotten are Incompatible with Free Speech », art. préc., p. 114 & 116-117.

515 J. Ausloos, « The "Right to be Forgotten" — Worth remembering », op. cit., p. 147.

516 V. supra, n° 7.

que du contexte[517], contribueraient à accroître la maîtrise sur les données personnelles. Il faudrait surtout insister sur le principe d'*accountability*. Selon l'article 22, § 1 de la proposition de règlement (« Obligations incombant au responsable du traitement »)[518], il faut entendre par principe d'*accountability* le principe en vertu duquel le « responsable du traitement adopte des règles internes et met œuvre les mesures appropriées pour garantir, et être en mesure de démontrer, que le traitement des données à caractère personnel est effectué dans le respect » des principes en matière de protection des données. Cela peut impliquer la tenue d'une documentation (art. 22, § 2, a)), la réalisation d'une analyse d'impact relative à la protection des données (art. 22, § 2, c)), la désignation d'une personne déléguée à la protection des données (art. 22, § 2, e)), etc. On ne peut ne pas songer, à cette évocation, au rôle que joue aujourd'hui la *Federal Trade Commission* et dont on a pu observer qu'il avait contribué à modifier les pratiques en matière de protection des données. Sans doute la solution sera-t-elle jugée très en retrait par rapport à celle d'un droit à l'oubli entendu comme « droit à l'effacement », mais elle a le mérite d'intégrer le monde des possibles du droit américain qui, comme dans le domaine des « principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée » (« *International Safe Harbor Privacy Principles* »)[519], s'accommode fort bien d'un mélange de règles de droit et d'autorégulation, de *hard*

517 Cf. J. Ausloos, art. préc. p. 150.

518 V. aussi : G29, Avis n° 3/2010 sur le principe de la responsabilité, 13 juill. 2010, 00062/10/FR WP 173.

519 En vertu de l'article 25, § 1 de la directive 95/46/CE, les Etats doivent veiller à ce que les transferts de données à caractère personnel vers un pays tiers n'aient lieu que si le pays tiers en question « assure un niveau de protection adéquat ». L'article 25, § 6 de la Directive permet à la Commission, assistée du comité établi en vertu de l'article 31 (groupe de l'article 29), de constater qu'un pays tiers assure un niveau de protection adéquat. En réaction à la directive et à ses exigences, le Department of Commerce américain, en particulier la National Information Agency, a rapidement affirmé que la volonté américaine était, en ce qui concerne du moins le secteur privé, d'assurer une protection adéquate dans le cadre non d'une législation, mais de codes de conduite et autres instruments d'autorégulation. Le résultat est l'élaboration des Safe Harbor Principles, c'est-à-dire, selon la traduction française, les « principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée ». Ces principes ont été adoptés par la Département américain du Commerce le 19 avril 1999 (« International Safe Harbor Privacy Principles », 19 avril 1999, http://www.ita.doc.gov/td/ecom/shprin.html) et accepté par la Commission européenne, en juillet 2000, soit deux ans après le début des négociations (Décision de la Commission du 26 juillet 2000, précitée). On trouve, dans ce texte, non seulement les principes de la sphère de sécurité, mais également des « Frequently Asked Questions » (FAQ - Foire Aux Questions) contenant des orientations importantes quant à la mise en œuvre des principes qui, il faut y insister, constituent le minimum devant être respecté par les entreprises et organisations américaines lors du transfert des renseignements personnels venant de l'Union européenne. Les principes sont les suivants : notification, choix, transfert des données (le transfert des données à des tierces parties n'est possible que si les tiers offrent un même niveau de respect des principes de protection des données personnelles), sécurité, accès, intégrité des données et mise en œuvre (« enforcement »). L'adhésion aux principes de la sphère de sécurité est volontaire. En cas d'autocertification, l'adhésion se fait sur la base d'une déclaration rendue publique sur le site du ministère du commerce américain. Par celle-ci, le responsable du traitement prend engagement de respecter les principes énoncés, à peine de sanction par la Federal Trade Commission. Le rôle d'exécution de la FTC repose sur le pouvoir général qu'elle tire de la section 5 du FTCA de sanctionner les actes et pratiques trompeuses et déloyaux. Pour une application, cf. In re Google Inc. (No. 102-3136, 2011 WL 1321658, *1, *2 (F.T.C. Mar. 30, 2011)). V., plus généralement, sur ces dispositions très complexes : Y. Poullet, « Les Safe Harbor Principles – Une protection adéquate ? », Colloque de l'IFCLA, Paris, 15 et 16 juin 2000 (http://www.droit-technologie.org/dossier-19/les-safe-harbor-principles-une-protection-adequate.html) ; pour une approche critique : D.J.B. Svantesson, « The regulation of cross-border data flows », IDPL 2011, Vol. 1, No. 3, p. 180 et s., spéc. p. 190 ; Ch. Connolly, Galexia, The US Safe Harbor – Fact or Fiction ?, Pyrmont (Australie), 2008, publié in Privacy Laws and Business International, issue 96, 2008, p. 1, 3, 26-27 ; R.H. Weber, « Transborder data transfers : concepts, regulatory approaches and new

law et *soft law*[520]. L'Union européenne serait bien avisée d'en tenir compte si elle ne veut pas proposer, en lieu et place d'une législation efficiente, à même de servir aussi de cadre à une réflexion plus globale sur la protection des données, un lit de Procuste qui deviendrait rapidement lit de mort de nos légitimes ambitions européennes.

---

initiatives », IDPL 2013, Vol. 3, No. 2, p. 117, spéc. p. 126 et s. ; pour une approche positive : D. Greer, « Safe Harbor – a framework that works », IJLIT 2011, Vol. 1, No. 3, p. 143 et s. (il importe de noter que l'auteur écrivait en qualité de responsable de l'administration du programme Safe Harbor auprès du Département américain du Commerce ; c'est une réponse partielle au rapport précité de Connoly, pour Galexia).

520 Il faut sans doute se souvenir de la formule de Whitman : à la différence des Européens, les Américains ont confiance dans le marché et non dans l'État (J.Q. Whitman, op. cit., p. 1189 ; v. aussi : F. Wero, op. cit., p 299).

CHAPITRE 3[1]

El derecho al olvido en internet: la experiencia española[2]

Introducción

Cancelar datos personales en Internet no resulta, de entrada, imposible: más bien todo lo contrario, constituye una práctica viable y habitual. La actividad supervisora de la Agencia Española de Protección de Datos (AEPD) lo demuestra y evidencia de forma incontestable a través de innumerables resoluciones que sancionan u obligan a los responsables de sitios de Internet a borrar datos que fueron almacenados sin la autorización de sus titulares.

Ahora bien, mayor dificultad plantea impedir que los motores de búsqueda de Internet indexen informaciones personales alojadas en sitios de Internet cuando así lo ordena la AEPD.

Google [3] se ha negado reiteradamente a ejecutar las Resoluciones de la AEPD y, con ello, a garantizar el derecho al olvido con fundamentos legales que sucintamente se resumen en los siguientes: 1) el rastreo automático del buscador se basa, primero, en la recolección de palabras clave, y, segundo, en la comparación de las palabras incluidas como criterio de búsqueda en la consulta del usuario con las de la lista; 2) el buscador es neutral a diferencia del titular del sitio web por ser el único capaz retirar la información; 3) la legislación española resulta inaplicable pues Google Spain se limita a representar a Google Inc. en la venta de publicidad como agente o representante mercantil exclusivo de Google Inc. pero sin responsabilidad sobre el buscador; 3´) los servicios de buscador los presta Google Inc. desde Estados Unidos sin que le sea de aplicación la directiva europea de protección de datos.

---

1 Texte traduit en français à l'Annexe 2

2 Par Artémi Rallo, Directeur honoraire de l'Agence espagnole de protection des données personnelles

3 El éxito planetario de los servicios ofrecidos por Google (en particular, de su motor de búsqueda) y sus recurrentes conflictos con la protección de la privacidad le han hecho acreedor de un tratamiento doctrinal profuso como lo demuestran, a modo de ejemplo, los siguientes trabajos: GOLDBERG M.A.: "The googling of online privacy: gmail, search-engine histories and the new frontier of protecting private information on the web", Lewis and Clark Law Review, vol. 9-1, 2005, págs. 249 a 272; CHURCH, P. and KON, G.: "Google at the heart of a data protection storm", Computer Law & Security Report, núm. 23, 2007, págs. 461 a 465; TENE, O.: "What Google knows: privacy and Internet search engines", Utah Law Review, núm. 4, 2008, págs. 1433 a 1492; MUTH, K.T.: "Googlestroika: Privatizing Privacy", Duquesne Law Review, vol. 47, 2009, págs. 337 a 353; DWYER, C.: "Privacy in the Age of Google and Facebook", IEEE Technology and Society Magazine, Fall, 2011, págs. 58 a 63; O'REILLY C.: "Finding jurisdiction to regulate Google and the Internet", European Journal of Law and Technology, vol. 2, núm. 1, 2011, págs. 1 a 13; RAKOWER, L.H.: "Blurred line: zooming in on google street view and the global right to privacy", Brooklyn Journal of International Law, núm. 37-1, 2011, págs. 317 a 347 ROSEN, J.: "The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google",Fordham Law Review, vol. 80-4, 2012,págs. 1525 a 1538.

No obstante, la AEPD ha construido unas bases jurídicas sobre las que sustentar el « modelo español" del derecho al olvido: 1') el derecho de oposición impide el tratamiento de datos personales cuando concurra un motivo legítimo y fundado referido a una concreta situación personal que lo justifique - arts. 18 Ley Orgánica de Protección de Datos (LOPD)-; 2') la legislación española resulta aplicable cuando el responsable del tratamiento no está establecido en territorio de la Unión Europea pero utiliza medios situados en territorio español; 3') la ley nacional española se aplicará cuando el tratamiento sea efectuado "en el marco de las actividades de un establecimiento » del responsable que implique el ejercicio efectivo y real de una actividad, independientemente de la forma jurídica del establecimiento (una oficina local, una filial con personalidad jurídica o una agencia de un tercero), como ocurre cuando se establece una oficina en un Estado miembro para la venta de publicidad orientada a los habitantes de este Estado; 4') los motores de búsqueda recurren a « medios » en el territorio del Estado miembro como, por ejemplo, los centros de almacenamiento de datos situados en el territorio del Estado, el uso de ordenadores personales, terminales y servidores o la utilización de cookies y programas informáticos similares.

Veamos, con mayor detenimiento, los argumentos expuestos por Google y cómo han sido rebatidos por la AEPD.

Section 1 - La pretensión de impunidad [4] de Google

I- La aplicación de la legislación estadounidense. Google inc como responsable exclusivo del buscador: ni establecimiento ni uso de medios en españa

Los servicios del motor de búsqueda de Google son de titularidad, prestación y responsabilidad única de Google Inc, - empresa estadounidense constituida conforme a las leyes de Delaware y con sede central en California – y, en consecuencia, cualquier controversia referida a las búsquedas (rastreo, almacenamiento, indexación o reclamaciones sobre protección de datos) se someterá exclusivamente a la legislación de EEUU y a la jurisdicción de California [5].

---

4 Como expresivamente afirma J. R. REIDEMBERG: "the initial wave of cases seeking to deny jurisdiction, choice of law, and enforcement to states where users and victims are located constitutes a type of "denial-of-service" attack against the legal system. Internet separatists use technology-based arguments to deny the existence of sufficient contacts for jurisdiction and the applicability of rules of law interdicting certain behavior. From this perspective, the attackers seek to disable states from protecting their citizens online" ("Technology and Internet Jurisdiction", University of Pennsylvania Law Review, vol. 153, 2005, pág. 1953).

5 Así lo proclaman las Condiciones de Servicio del buscador Google en su versión de 1 de marzo de 2012: "En algunos países, los tribunales no aplicarán las leyes del estado de California (Estados Unidos) para solucionar algunos tipos de controversias. Si resides en uno de esos países, al no regir las leyes de California, se aplicará la ley de su país en los conflictos relacionados con estas condiciones. De lo contrario, aceptas que las leyes del estado de California (Estados Unidos), excluyendo las disposiciones sobre conflicto de leyes, se apliquen a cualquier conflicto que se derive de estas condiciones o de los Servicios o que esté relacionado con los mismos. Del mismo modo, si las leyes

Google Spain es una mera empresa filial de Google Inc cuya actividad se limita a la prestar servicios de marketing de la venta de publicidad en España y, en consecuencia, no presta servicio alguno sobre el buscador pues no dispone de capacidad alguna a tal efecto.

Sobre las dos premisas anteriores y al amparo de la dispersión de criterios resolutivos contrarios [6] y favorables [7] a la aplicabilidad de la legislación europea al buscador, Google niega que Google Spain pueda ser considerada un establecimiento de la compañía ubicado en España y, conforme las reglas de aplicabilidad territorial establecidas en los arts. 4. 1 a) de la Directiva 95/46 y 2.1 a) LOPD, deriva toda la responsabilidad sobre la actividad del buscador hacia Google Inc. en el marco exclusivo de la legislación estadounidense.

Tampoco Google admite el « recurso a medios ubicados en España » para la prestación de su servicio de buscador. Google Inc. prestaría dicho servicio global por medio de centros de datos – ninguno de ellos situado en España - a los que los usuarios españoles transferirían sus datos. Los

---

de tu país no te permiten someterte a la jurisdicción de los tribunales del condado de Santa Clara (California, EE.UU.), los litigios relacionados con estas condiciones se someterán a la jurisdicción y a los poderes locales. En caso contrario, tanto Google como tú aceptáis someteros a la jurisdicción exclusiva de los tribunales federales o estatales del condado de Santa Clara (California, Estados Unidos) para solucionar las reclamaciones derivadas de estas condiciones o de los Servicio o relacionadas con los mismos"
(https://www.google.es/intl/es/policies/terms/regional.html).

6 En buena parte de los procedimientos resueltos por la AEPD, Google argumentó su posición acudiendo a la posición mantenida por otras autoridades nacionales administrativas y judiciales: 1') Una resolución del Garante Italiano para la Protección de Datos, de 11 de diciembre de 2008, que inadmitía una petición de cancelación de datos de un particular por entender que Google Inc no estaba ubicada en ningún Estado miembro de la Unión Europea y su tratamiento de datos se realizada mediante servidores ubicados en EEUU. 2') Una Sentencia del Tribunal de Gran Instancia de Paris, de 14 de abril de 2008, denegó las pretensiones de un particular contra Google Inc. y Google France al entender que el servicio de búsquedas lo prestaba exclusivamente Google Inc., sin establecimiento ni uso de medios en Francia, mientras que Google France actuaba solo como agente comercial. 3') Una sentencia de un Juzgado de Primera Instancia de Bruselas, de 2 de junio de 2009, rechazó la demanda contra Google Belgium atribuyéndole la facultad de cancelar los resultados de búsqueda a Google.

7 Sin embargo, las resoluciones anteriores, traídas a colación para negar la aplicación de la legislación europea al buscador Google, quedan desdibujadas por otras muchas en las que autoridades nacionales administrativas y judiciales sí estimaban aplicable la legislación europea al buscador Google en litigios referidos a la función "autocompletar": 1º) por supuesto, la AEPD en su Resolución 2647/2012 (TD/1105/2012) estimó una demanda contra Google Spain instándole a adoptar las medidas necesarias para evitar la asociación indebida de los datos de un reclamante con el término "gay" en sus índices de sugerencia producidos por la función Autocompletar; 2º) con anterioridad, una Sentencia de la Cour d´Appel de Paris, de 18 de diciembre de 2011, recaída en un litigio entre Google y la aseguradora Lyonnaise de Garantie, estimó que, habiendo quedado ampliamente acreditado mediante notificaciones específicas el conocimiento real y no proceder Google a retirar las sugerencias – en concreto, el nombre de la aseguradora se asociaba al término francés « scroc » (estafa)- de la función autocompletar, debía multarla y ordenar la retirada de la sugerencia automatizada; 3º) en supuesto similar, un Tribunal Ordinario de Milán dictó Sentencia, el 24 de marzo de 2011, ordenando a Google retirar de la función Autocompletar la sugerencia que asociaba al reclamante con los términos italianos « truffatore »(estafador) y « truffa »(estafa); 4º) más recientemente, en abril de 2013, un Tribunal japonés condenó a Google por asociar en sus sugerencias de la función autocompletar el nombre de un ciudadano al de un grupo criminal; 5º) y, en mayo de 2013, el Tribunal Supremo de Alemania obligó a Google a eliminar de su buscador las sugerencias automáticas que asociaban en la función autocompletar el apellido de un empresario con los términos « cienciología » y « estafa » (El País, 15 de mayo de 2013, pág. 52).

« robots » o « arañas » estarían ubicados en dichos centros donde rastrearían la información de Internet solicitando, obteniendo la información de las webs – si el webmaster responsable de la información autoriza el envío- e indexándola de forma automatizada. De forma que todos los procesos relativos a la actividad de los buscadores se realizarían en los equipos informáticos de Google allí donde se encuentren pero sin utilizar medios técnicos donde se aloja en origen la información.

En consecuencia, tampoco resultaría territorialmente aplicable la legislación europea o española al no « recurrir a medios ubicados » en España para realizar el tratamiento de datos en los términos previstos por los arts. 4. 1 a) de la Directiva 95/46 y 2. 1 c) LOPD.

II - La neutralidad del automatismo de los buscadores como presupuesto de la irresponsabilidad. El webmaster como exclusivo responsable directo

La neutralidad del servicio de búsqueda constituye, sin duda, uno de los principales asideros sobre los que Google argumenta su falta de responsabilidad sobre el tratamiento de datos que implica la actividad del buscador. Por el contrario, la capacidad del webmaster de decidir sobre la indexación de los contenidos de su web le convertiría en responsable directo y, en consecuencia, debería garantizar el cumplimiento de la normativa de protección de datos.

El buscador de Google, como los restantes, realizaría el proceso de obtención de información de forma similar a como lo hacen los usuarios de Internet: formularía automatizadamente, mediante el rastreo de sus robots o arañas, una petición a los servidores que la alojan y éstos admitirían o no su acceso, total o parcial, según las propias instrucciones prefiguradas, esto es, el webmaster o quien publica la información decidirían si el servidor de alojamiento de la web envía la información solicitada y, en ningún caso, el buscador extraería información de los servidores ni accedería a los mismos sin que el webmaster lo posibilitara.

En definitiva, Google eludiría cualquier responsabilidad al considerar que las decisiones sobre la finalidad y destino de la información personal corresponderían exclusivamente a los webmaster que posibilitan el acceso a la información y a terceros que la replican. Esto es, solo ellos decidirían sobre los fines y los medios de datos [arts. 2 d) Directiva 95/46 y 3 d) LOPD].

En su favor, Google hace valer el *Dictamen 1/2008 sobre motores de búsqueda en Internet*, de 4 de abril de 2008, del Grupo de Trabajo del Art. 29 en el que se diferenciaría el grado de responsabilidad del webmaster y del buscador negándole a éste la responsabilidad principal por los datos objeto de tratamiento y atribuyéndosela al responsable de la web en la que se publicó la información personal: « El principio de proporcionalidad requiere que, en la medida en que un proveedor de un motor de búsqueda actúe exclusivamente como intermediario, no debe considerarse como responsable principal del tratamiento de datos personales efectuado. En este caso, los responsables principales del tratamiento de datos personales son los proveedores de información »[8]. Sin embargo, Google no advierte que esta misma cita va acompañada de una

8http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

directa responsabilidad de los buscadores referida a la retirada de datos personales de su índice: « La responsabilidad formal, jurídica y práctica de los datos personales que incumbe al motor de búsqueda se limita generalmente a la posibilidad de retirar datos de sus servidores. Por lo que se refiere a la retirada de datos personales de su índice y de sus resultados de búsqueda, los motores de búsqueda tienen una responsabilidad suficiente para considerarse responsables del tratamiento (solos o conjuntamente con otros) » cuando exista una obligación de retirar o bloquear datos personales derivada de la legislación de Estados miembros[9].

III - La ineficacia del derecho al olvido exclusivamente ejercido ante los buscadores de internet y el principio de proporcionalidad

Google advierte que la pretensión de una autoridad administrativa consistente en dirigirse exclusivamente al buscador para ordenar la retirada de sus índices de una información personal resultará inoperante si, previamente, el webmaster que publicó la información no la suprime y/o introduce herramientas técnicas que obstaculicen su indexación. Además, pudiendo evitar el acceso del buscador Google, si dicha información permanece en la web podrá seguir resultado accesible para cualquier otro buscador o plataforma de Internet y, en consecuencia, resultará de acceso público.

Google apela a la necesidad de atender al principio de proporcionalidad, como principio fundamental del Derecho Comunitario – « En virtud del principio de proporcionalidad, el contenido y la forma de acción de la Unión no excederá de lo necesario para alcanzar los objetivos de los Tratados » (art. 5.4 Tratado de la Unión Europea)-, para enjuiciar las resoluciones de la AEPD de conformidad con la legislación y jurisprudencia europea y las libertades de expresión, información y empresa (arts. 11 y 16 Carta de Derechos Fundamentales de la Unión Europea).

Google niega a la AEPD habilitación en el Derecho español para resolver el derecho de oposición que obliga a Google a eliminar información de su buscador mediante una ponderación de diversos derechos fundamentales en liza: la privacidad y dignidad del reclamante, la libertad de expresión e información de quien publica la información y de terceros usuarios que potencialmente podrían acceder a ella y la libertad de empresa del buscador.

Sin embargo, como recuerda Google, la reciente jurisprudencia europea – referida a la protección del derecho de autor frente a las descargas ilegales en Internet - obliga a las autoridades nacionales a realizar una ponderación entre todos estos derechos en conflicto "el Derecho

---

9 En particular, el Dictamen 148 cita en su nota a pie de página núm. 18 el caso español: « En algunos Estados miembros de la UE, las autoridades de protección de datos han regulado específicamente la obligación de los proveedores de motores de búsqueda de retirar datos de contenido del índice de búsqueda, sobre la base del derecho de oposición consagrado en el artículo 14 de la Directiva sobre protección de datos (95/46/CE) así como en la Directiva sobre el comercio electrónico (2000/31/CE). En virtud de estas legislaciones nacionales, los motores de búsqueda se ven obligados a seguir una política de notificación y retirada similar a la seguida por los proveedores de servicios de alojamiento, con el fin de evitar la responsabilidad ».

comunitario exige que dichos Estados miembros, a la hora de adaptar su ordenamiento jurídico interno a estas Directivas, procuren basarse en una interpretación de éstas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también no basarse en una interpretación de éstas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad"[10]. En particular, el TJUE ha especificado: «las autoridades y órganos jurisdiccionales nacionales deben garantizar, en particular, un justo equilibrio entre la protección del derecho de propiedad intelectual que ampara a los titulares de derechos de autor y la protección de la libertad de empresa que ampara a los operadores, como los PAI (proveedores de acceso a Internet), en virtud del art. 16 de la Carta »[11].

Como resulta obvio, el principio de proporcionalidad está presente en la resolución de numerosas cuestiones prejudiciales presentadas ante el TJUE cuya resolución ha implicado la necesaria ponderación entre medios utilizados y fines a alcanzar para proteger derechos fundamentales que, en ningún caso, ninguno de ellos, son absolutos como lo reitera el Tribunal de Justicia de la Unión Europea (TJUE) en relación al derecho a la protección de datos (y, en otros supuestos, lo hace de tantos otros derechos fundamentales). Sin embargo, para Google la correcta aplicación del principio de proporcionalidad en este litigio sobre del derecho al olvido frente a los buscadores exige partir de las siguientes premisas: 1) la exactitud de sus índices sobre los contenidos indexados de las webs; 2) la actualización automática y continua de los índices para preservar dicha exactitud en la información; 3) la excesiva gravosidad de los medios (la retirada directa de los contenidos en los índices del buscador) que se pretenden utilizar para evitar la accesibilidad a informaciones lícitamente publicadas en webs de Internet.

La conclusión de Google es contundente: obligarle a suprimir en sus índices enlaces a webs resultaría ineficaz, ineficiente y desproporcionado por las siguientes razones: 1) porque resultaría mucho menos costoso y más eficaz para satisfacer el derecho al olvido que el webmaster utilizara los medios de que ya dispone para evitar enlaces no sólo a un concreto buscador sino a cualesquiera otros y restantes aplicaciones existentes en Internet; 2) porque, con la intervención limitadora del webmaster, los ciudadanos no se verían obligados a identificar la pluralidad de buscadores, webs, redes, etc. en que se alojaría su información y bastaría con un único ejercicio de sus derechos; 3) porque la eliminación de enlaces y referencias en los índices del buscador no sólo supondría suprimir específicas referencias personales sino páginas completas de Internet desvirtuando progresivamente la utilidad del buscador y quebrando su función nuclear en el avance de la sociedad de la información y del conocimiento; 4) porque la eliminación de resultados de búsquedas quebraría, entre otros, el derecho a la información tanto de quienes la publican como del resto de usuarios que ostentarían un hipotético derecho fundamental a acceder a dicha información.

---

10 STJUE de 29 de enero de 2008, Caso Promusicae vs. Telefónica, C-275/06.

11 STJUE, de 24 de noviembre de 2011, Caso SABAM, C-70/2010.

Section 2- La AEPD defiende el derecho de oposición como derecho al olvido en el actual estado tecnologico de los buscadores de internet

I- La aplicación de la legislación española al buscador de internet (i): Google spain como « establecimiento » de Google inc en españa

Frente a la negativa de Google Spain a reconocer responsabilidad alguna por la prestación del servicio de búsquedas –alegando que dichos servicios son prestados por Google Inc y que, en consecuencia, no les resulta de aplicación ni la Directiva europea 95/46 ni la legislación española de protección de datos -, por tratarse de una empresa que limita su actividad a promocionar la venta de publicidad anexa a las búsquedas, la AEPD ha afirmado lo contrario en base a los argumentos siguientes.

El art. 2.1 a) LOPD somete a dicha norma a todo tratamiento de datos de carácter personal « cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento », esto es, esta norma traspone la Directiva 95/46 de protección de datos que, sobre el Derecho nacional aplicable, proclama que los Estados miembros aplicarán las disposiciones nacionales que hayan aprobado para la aplicación de la Directiva a todo tratamiento de datos personales cuando:

> « El tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable » [art. 4.1 a)].

Por lo tanto, la legislación española se aplicaría, según el art. 4.1 a) de la Directiva 95/46, a Google Spain si fuera considerado el "establecimiento" en el marco de cuyas actividades se realiza en territorio español el tratamiento de datos por el buscador. En otras palabras, ¿es Google Spain el "establecimiento" responsable en España del tratamiento de datos realizado por el buscador?

La respuesta al interrogante anterior obliga a realizar un ejercicio interpretativo que tenga en cuenta los textos que sirven principalmente a la interpretación de la Directiva 95/46, esto es, los Considerandos que acompañan a los preceptos que la integran y, en segundo lugar, no menos relevante, los Dictámenes elaborados por el Grupo de Trabajo integrado por todas las Autoridades de Protección de Datos de la Unión Europea y creado por el art. 29 de la Directiva 95/46, precisamente, para dicha finalidad consultiva.

En primer lugar, resulta relevante - para determinar la voluntad del legislador europeo sobre el alcance de la aplicabilidad territorial de las legislaciones nacionales para otorgar una garantía efectiva de derechos - enjuiciar si nos hallamos ante un "establecimiento" en el sentido del art. 4. 1 a) de la Directiva y, a estos efectos, constituye recurso obligado reproducir lo establecido en el Considerando (18):

« Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado ».

En segundo lugar, resultará determinante para evaluar si, en el caso de Google Spain, nos hallamos ante un "establecimiento" en el sentido del art. 4. 1 a) de la Directiva, el recurso a lo establecido en el Considerando (19):

« Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades ».

Como puede observarse, ambos Considerandos están presididos por la intención de otorgar garantía efectiva al derecho de protección de datos: por un lado, confirmando la ineludible exigencia de que todo tratamiento de datos efectuado en el territorio europeo esté sometido a la legislación de alguno de los Estados miembros; por otro, huyendo de formalismos que permitan eludir a quien decide sobre dicho tratamiento la aplicación normativa de la legislación nacional.

El antiformalismo presente en el considerando (19) de la Directiva 95/46 lleva a atribuir la condición de "establecimiento" a la entidad que, mediante una instalación estable, ejerce una actividad de forma efectiva y real - independiente de la forma jurídica que ostente: mera sucursal o filial con personalidad jurídica -. Se trata, sin duda, de una ineludible aproximación al concepto de "establecimiento" requerida en el complejo y heterogéneo mundo actual de la sociedad de la información y del conocimiento en que, de forma especial, las empresas multinacionales que operan en Internet ofrecen las más diversas modalidades de personación en el ámbito local y, la mayor parte de las veces, tratan de eludir su alcance globalizador con un sometimiento a la legislación estadounidense que busca rehuir a aplicación de la legislación de los países en los que operan.

Los motores de búsqueda, lejos de ser ajenos a la problemática anterior, la ejemplifican de forma paradigmática y, para desentrañar la maraña jurídico-formal que el Considerando 19 de la Directiva aventura, debe recurrirse al Dictamen 1/2008, de 4 de abril, sobre buscadores de Internet [12], donde el Grupo de Trabajo del Art. 29 fijó algunos criterios que permiten concluir

12 Recuérdese que el referido Dictamen declaró aplicable a los buscadores la legislación europea y, como derivada, les impuso una reducción significativa de los periodos de conservación de datos. Al respecto, véase KOSTA, E., KALLONIATIS, Ch., MITROU, L. Y KAVAKLI, E.: "The "Panopticon" of search engines: the response of the European data protection framework", Digital Privacy, Springer, vol. 16, 2010, págs. 47 a 54.

cuándo existe un "establecimiento" –al margen de su forma jurídica- por desempeñar un papel significativo:

1) cuando un proveedor de motor de búsqueda establece una oficina en un Estado miembro (EEE) que participa en la venta de publicidad orientada a los habitantes de este
Estado;
2) cuando un establecimiento es responsable de las relaciones con los usuarios del motor de búsqueda en una jurisdicción determinada;
3) cuando el establecimiento de un proveedor de motor de búsqueda respeta las resoluciones de los tribunales y/o responde a las solicitudes de las autoridades competentes de un Estado miembro respecto a los datos de los usuarios.

La AEPD ha acumulado indicios que evidencian la concurrencia en Google Spain de estos tres criterios para determinar su naturaleza como establecimiento ubicado en España responsable del buscador.

En primer lugar, resulta evidente que la publicidad es la forma de financiación del buscador Google sin que el usuario pueda evitarla si quiere utilizar el servicio del buscador y el tratamiento de datos que realiza Google va dirigido a prestar servicios a los usuarios entre los que destaca la publicidad personalizada [13]. Obviamente, la publicidad vinculada al servicio de búsqueda y dirigida específicamente al territorio español se asienta en la actividad de Google Spain. Por lo tanto, siendo la actividad económica realizada en territorio español por Google Inc la generación de publicidad insertada en el servicio gratuito de búsquedas, hay que concluir que para dicha actividad utiliza promotores locales como Google Spain que incentivan la compra de espacios publicitarios.

En segundo lugar, frente a la alegación habitual de Google Spain afirmando que su representación en España Google se limita a la promoción de la venta de publicidad y que ninguna responsabilidad ostenta sobre el cumplimiento de la normativa de protección de datos, la AEPD ilustra numerosas resoluciones con datos que evidencian la representación de Google Inc por Google Spain en diversos procedimientos tramitados por la AEPD. Así, Google Spain ha atendido numerosos requerimientos que le han sido dirigidos por la Subdirección de Inspección de la AEPD en la tramitación de procedimientos de tutelas de derechos respecto de reclamaciones formuladas por ciudadanos españoles en relación al servicio de búsqueda [14].

En tercer lugar, lejos de limitar su actividad a la promoción de la venta publicitaria, Google Spain extiende su representación de Google Inc en España a la promoción e, incluso, resolución de controversias sobre protección de datos relativas a otros servicios de Google. Sirvan como

---

13 El sistema AdWords ofrece publicidad a partir de los resultados de las búsquedas realizas por el propio usuario atendiendo, especialmente, a su vinculación territorial. De hecho, a las empresas anunciantes se les solicita que definan sus potenciales consumidores en función del país al que se orientan. El sistema de publicidad AdSense rastrea automáticamente el contenido de las páginas y publica anuncios relevantes para los usuarios ubicados en territorio español.

14 TD/299/2007, TD/463/2007, TD/814/2007, TD/155/2008, TD/387/2008, TD/420/2008, TD/444/2008, TD/569/2008 y TD/580/2008.

ejemplo las alegaciones presentadas por Google Spain en el expediente de actuaciones previas de inspección E/01544/2007, tramitado como consecuencia de una denuncia presentada por una organización de usuarios española, en relación con el servicio de correo electrónico gratuito "Gmail". También resulta notoria la intermediación de Google Spain actuando como representante de Youtube a la vista de las declaraciones promocionales de sus directivos en los medios de comunicación.

En cuanto lugar, tanto Google Inc como Google Ireland tienen designada en los ficheros declarados ante el Registro General de Protección de Datos de la AEPD a Google Spain como la entidad que atiende el ejercicio de los derechos de acceso, rectificación, cancelación y oposición previstos en la LOPD.

Todo lo anterior, lleva a la AEPD a concluir favorablemente la condición de Google Spain como representante en España de Google Inc actuando como establecimiento del responsable del servicio de búsqueda.

II- La aplicación de la legislación española al buscador de internet (II): Google « usa medios » ubicados en españa

La aplicación de la legislación española de protección de datos puede traer causa, alterantiva o acumulativamente, de un segundo criterio. El art. 2.1 c) LOPD obliga a la vigencia de esta norma sobre los tratamientos de datos "cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito". Este precepto traspone la Directiva 95/46 de protección de datos que también preceptúa la aplicación de la legislación nacional a todo tratamiento de datos personales cuando:

> « 1...c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea. 2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento » (art. 4) [15].

Para determinar la voluntad del legislador europeo sobre la aplicabilidad territorial de la legislación española a las actividades del buscador por utilizar medios situados en un Estado miembro, hay que estar a lo que, sobre los arts. 4. 1 c) y 2 de la Directiva, establece el Considerando (20):

---

15 Un exhaustivo análisis sobre este precepto y, en particular, sobre su iter legislativo, en MOEREL, L.: "The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", International Data Privacy Law, vol. 1, no. 1, 2011, págs. 28 a 46.

« Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adaptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva ».

Con este nuevo criterio, la Directiva 95/46 complementa el enfoque antiformalista que preside el concepto de "establecimiento" con una aproximación teleológica que pone de relieve las finalidades a las que sirve la Directiva 95/46 y que no pueden desvirtuarse a causa de la naturaleza transnacional de numerosos servicios de Internet. Esto es, este Considerando (20) constata la habitual existencia en el entorno de Internet de responsables de servicios ubicados en países terceros (de nuevo, principalmente, Estados Unidos) y advierte que dicha práctica "no debe obstaculizar" la protección de los derechos individuales. Por ello, se reafirma la vigencia de la legislación de aquellos Estados miembros en los que se ubiquen medios para el tratamiento de los datos personales y se conmina a la "adaptación" de las garantías previstas en la normativa de protección de datos para que se respeten "en la práctica" los derechos y obligaciones previstos en la Directiva. En fin, la aproximación normativo-formalista anclada en las categorías tradicionales de articulación de las relaciones responsabilidades transnacionales debe dejar paso a una visión realista-material que anteponga, en la práctica, la garantía efectiva de los derechos en juego frente a actitudes elusivas u obstaculizadoras.

Dicho lo anterior, tampoco se deduce expresamente de la Directiva 95/46 cuándo hay que entender que los servicios de búsqueda de Internet utilizan "medios" ubicados en un Estado miembro por lo que, de nuevo, resulta de inestimable ayuda el recurso a los Dictámenes del Grupo de Trabajo del Art. 29.

En concreto, ya el 30 de mayo de 2002 se adoptaba el *Documento de Trabajo núm. 56, relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE*, donde se ilustraba la casuística de "medios" ubicados en territorio de Estados miembros a los que resultaría aplicable el art. 4.1 c) de la Directiva 95/46: "Los PC, los terminales y los servidores, que se pueden utilizar para casi todos los tipos de operaciones de tratamiento de datos, son ejemplos de 'medios'... Un ejemplo típico de medios utilizados exclusivamente para el tránsito son las redes de telecomunicaciones (ejes centrales, cables, etc.), que forman parte de Internet y por las cuales pasan las comunicaciones Internet desde el punto de expedición hasta el punto de destino ... no es necesario que el responsable del tratamiento tenga un control total sobre los medios. El responsable del tratamiento puede tener un control variable de estos medios. El control es suficiente cuando el responsable del tratamiento, al determinar la forma en que estos medios funcionan, toma las decisiones adecuadas en relación con la naturaleza de los datos y su tratamiento. En otras palabras, el responsable determina qué datos se recogen, se almacenan, se transfieren, se modifican, etc., de qué forma y con qué objetivo ... el concepto de «recurrir» presupone dos elementos: un determinado tipo de actividad emprendida por el responsable y su intención de tratar datos personales...la facultad de disposición del responsable no debe confundirse con la propiedad o la posesión de los medios, ya sea por el responsable del

tratamiento, o por la persona. De hecho, la Directiva no concede ninguna importancia a la propiedad de los medios"[16].

Como puede observarse, resulta obligado un análisis doble: por un lado, sobre los elementos tecnológicos que integran el concepto de equipamiento utilizado para el tratamiento de datos por el responsable; y, por otro lado, la naturaleza jurídico-formal de dichos medios que evidencia el relativismo con el que hay que acudir para evaluar el nivel de « control o titularidad » que el responsable puede ejercer sobre dichos medios.

Pero, bebiendo del documento anterior, de nuevo será el *Dictamen 1/2008, de 4 de abril, sobre buscadores de Internet* el que emita conclusiones específicas sobre la aplicabilidad de la legislación nacional a los buscadores de Internet por utilización de medios ubicados en Estado miembros. Como afirma este documento, siendo práctica habitual, cuando la prestación de servicios de motor de búsqueda se realiza desde fuera de la Unión Europea, habrá que considerar como tales medios los siguientes:

1) los centros de datos situados en el territorio de un Estado miembro pueden utilizarse para el almacenamiento y el tratamiento a distancia de datos personales;
2) el uso de ordenadores personales, terminales y servidores;
3) la utilización de cookies y de programas informáticos similares[17].

A la vista de los criterios interpretativos enumerados, la AEPD ha profundizado en el análisis sobre cómo el buscador de Google dirige sus servicios específicamente al territorio español [18] y sobre las circunstancias que ilustran la utilización por el buscador de Google de medios ubicados en España.

16http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

17 Como recuerda el Dictamen 1/2008, ya el Documento de Trabajo núm. 56 del Art. 29 concluía: "el PC del usuario puede considerarse un «medio» con arreglo a la letra c) del apartado 1 del artículo 4 de la Directiva 95/46/CE. Está ubicado en el territorio de un Estado miembro. El responsable decidió utilizarlo para el tratamiento de datos personales y, tal como se explica en los apartados anteriores, tienen lugar varias operaciones técnicas sin un control por parte del interesado. El responsable del tratamiento emplea los medios del usuario y no lo hace solamente con fines de tránsito en el territorio de la Comunidad. El Grupo de Trabajo opina por lo tanto que las condiciones en que pueden recogerse datos personales del usuario mediante la colocación de cookies en su disco duro son reguladas por el Derecho nacional del Estado miembro donde se sitúa este ordenador personal".

18 La STJUE, de 7 de diciembre de 2010 (C-585/08 y C-144/09), Pammer vsReederei Karl Schlüter GmbH & Co KG y Hotel Alpenhof GesmbH vs Oliver Heller, nos ilustra sobre elementos que, con carácter no exhaustivo, pueden constituir indicios que permiten considerar que determinada actividad está dirigida al Estado miembro del domicilio del consumidor: "el carácter internacional de la actividad, la utilización de una lengua distinta de la habitualmente empleada en el Estado miembro en el que está establecido el vendedor, la mención de números de teléfono con indicación de un prefijo internacional, la utilización de un nombre de dominio de primer nivel distinto al del Estado miembro en que está establecido el vendedor y la mención de una clientela internacional formada por clientes domiciliados en diferentes Estados miembros. Corresponde al juez nacional comprobar si existen esos indicios. En cambio, el mero hecho de que pueda accederse a la página web del vendedor o del intermediario en el Estado miembro del domicilio del consumidor es insuficiente. Lo mismo ocurre con la mención de una dirección electrónica y de otros datos o con la utilización de una lengua habitualmente empleada en el Estado miembro en el que está establecido el vendedor".

En primer lugar, como es sabido, el servicio de búsqueda se presta a nivel mundial con la web www.google.com pero existen infinidad de versiones nacionales que utilizan el idioma nacional (o, incluso, varios de ellos) y a las que, por defecto, se accede atendiendo a la ubicación geográfica del usuario. En España, este servicio de búsqueda se ofrece en el sitio google.es. Los servidores web ubicados en España son visitados por el buscador de Google para alimentar su almacenamiento de información y, posteriormente, ofrecer sus resultados, especialmente, a los usuarios españoles. La información rastreada, almacenada e indexada por el buscador desde servidores ubicados en España hará referencia tanto a datos de usuarios como de terceros. El idioma utilizado en los documentos o en los servidores web que los alojan resulta determinante en la acción de rastreo del buscador puesto que, de hecho, el usuario decide si los resultados de su búsqueda se refieran a páginas ubicadas en España. Para ofrecer esta posibilidad el buscador necesita acceder a servidores web españoles y almacenar los resultados del rastreo para ofrecerlos al usuario ubicado en España -todo ello, lógicamente, tras utilizar medios técnicos ubicados en territorio español.

En segundo lugar, la AEPD enfatiza que el servicio de búsqueda de Google prestado a través de google.es está específicamente dirigido al territorio español atendiendo a los siguientes elementos: 1) El idioma utilizado en google.es es el castellano aunque se admiten, incluso, versiones en catalán, euskera y gallego. 2) El dominio utilizado por el buscador Google en España (google.es) es un dominio territorial registrado en Red.es bajo el código de país correspondiente a España. 3) Los resultados de las búsquedas indexados en google.es se dirigen, básicamente, a usuarios ubicados en el territorio español. 4) Google se financia a través de publicidad anexada a resultados de búsquedas que evidencian su vinculación específica al territorio español.

III- La aplicación de la legislación española al buscador de google (III): directiva 2000/31 y ley de servicios de la sociedad de la información

El recurrente debate sobre la aplicación de la legislación de protección de datos a los servicios de búsqueda de internet de empresas ubicadas fuera de la Unión Europea desconoce, en ocasiones, la existencia de leyes específicas dirigidas a estos servicios de la sociedad de la información que no dejan margen a la duda sobre la aplicación a los mismos de la legislación nacional y, específicamente, española.

Así, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) – trasponiendo la Directiva 2000/31 relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior - establece en su art. 4 que los prestadores que dirijan sus servicios específicamente al territorio español – que, al entender de la AEPD sería el caso del buscador de Google – "quedarán sujetos a las obligaciones previstas en esta Ley, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicables". En concreto, el art. 8.1 c) LSSI añade: « En caso de que un determinado servicio de la sociedad de la información atente

o pueda atentar contra *el respeto a la dignidad de la persona* [19], los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados ».

Lejos, por tanto, de amparar la impunidad de los buscadores de Internet, la LSSI los somete a las obligaciones previstas en dicha norma cuando dirigen sus servicios al territorio español y, tan es así, que prevé la posibilidad de que las autoridades competentes puedan interrumpir sus servicios o retirar aquellos datos que resulten ilícitos por contravenir los principios referidos en la LSSI como es el caso el respeto a la dignidad humana. La AEPD no duda en atribuirse la condición de autoridad nacional habilitada por la legislación española para acordar la interrupción de servicios de la sociedad de la información o la retirada de datos que conculquen el respeto debido a la dignidad humana y, en consecuencia, a los derechos fundamentales que les son inherentes (art. 10.1 CE) de entre los que resultará especialmente concernido el derecho fundamental a la protección de datos personales.

En concreto, las muchas resoluciones de la AEPD recaídas para la tutela del derecho al olvido ante los buscadores de Internet gustan traer a colación relevante jurisprudencia constitucional que reafirma la conexión entre *la dignidad humana* y la protección de datos: « el artículo 18.4 de la Constitución Española contiene ... un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática' ... el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado » (STC 292/2000).

IV - La responsabilidad de google tras el « conocimiento efectivo » de la ilicitud de las búsquedas

Declarar la aplicabilidad de la legislación española a la actividad de búsqueda de Google no resuelve el interrogante principal sobre el alcance de su responsabilidad en el tratamiento de las informaciones personales indexadas frente a una hipotética ilicitud de las mismas.

---

19 Los principios cuya conculcación puede llevar a los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, a adoptar las medidas necesarias para interrumpir su prestación o para retirar los datos que los vulneran son: ") La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional. b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores. c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social. d) La protección de la juventud y de la infancia. e) La salvaguarda de los derechos de propiedad intelectual".

La Directiva 2000/31, de 8 de junio de 2000, sobre el comercio electrónico, resulta terminante al declarar, en términos generales, la inexistencia de obligación general de supervisión en su art. 15.1: « 1. Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas ».

De nuevo, la LSSI ilustra esta cuestión al trasponer la referida Directiva y regular en su art. 17 el régimen de « responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda »[20]:

1) Como regla general, el art. 17 LSSI exonera de responsabilidad por los datos que difunden a « los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos » (en definitiva, en general, a los motores de búsqueda de Internet y, en particular, a Google Search).

2) Sin embargo, la responsabilidad del buscador por los resultados de las búsquedas aflorará en el momento en que concurran dos condiciones:

1ª) que tenga conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización;

2ª) y, si lo tienen, no actúen con diligencia para suprimir o inutilizar el enlace.

Los buscadores de Internet, en tanto servicios de intermediación que no ofertan contenidos propios sino ajenos, no tienen *a priori*[21] responsabilidad alguna por los contenidos que rastrean, almacenan, indexan y difunden por Internet. Esto es, el tratamiento automatizado que realizan los buscadores de Internet no genera responsabilidad *per se* hasta el momento en que la neutralidad que acompaña al automatismo cede al singular conocimiento y aparecen las responsabilidades

---

20 En casi idénticos términos el art. 14 de la Directiva 2000/31 establece: "1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que: a) el prestador de servicios no tenga conocimiento efectivo de que la actividad a la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o de que, b) en cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible".

21 Resulta de interés advertir que la STJUE (C-70/2010, STJUE de 24 de noviembre de 2011) del Caso SABAM rechaza obligar a determinados servicios de la sociedad de la información a un "filtrado indiscriminado y preventivo" de los contenidos que alojan tras un análisis conjunto de las Directivas 2000/31, 2001/29 y 2004/48. Las Directivas, interpretadas a la luz de los requisitos derivados de la protección de los derechos fundamentales aplicables, deben interpretarse en el sentido de que se oponen a un requerimiento judicial hecho por un juez nacional por el que se ordene a un prestador de servicios de alojamiento de datos establecer un sistema de filtrado: 1´) de la información almacenada en sus servidores por los usuarios de sus servicios; 2´) que se aplique indistintamente con respecto a toda su clientela; 3´) con carácter preventivo; 4´) exclusivamente a sus expensas; y 5´) sin limitación en el tiempo".

jurídicas derivadas de obligaciones legales que buscan preservar la garantía de los derechos fundamentales [22].

La responsabilidad del buscador emerge, por lo tanto, cuando concurren tres requisitos que deberán sucederse en el tiempo: 1°) « ilicitud declarada de la información », 2°) « conocimiento efectivo » ; 3°) y « falta de diligencia » en su retirada.

El art. 17 LSSI aporta, además, dos elementos adicionales para aclarar el alcance de dichos requisitos:

1) por un lado, fija el « conocimiento efectivo » en el momento en que el prestador de servicios conoce la resolución del órgano competente en la que se haya declarado la ilicitud de los datos, ordenado su retirada o la imposibilidad de acceso a los mismos, o se hubiera declarado la existencia de la lesión;

2) por otro lado, nada impide que el prestador del servicio pueda adquirir un « conocimiento efectivo » aplicando sus acuerdos voluntarios de detección y retirada de contenidos.

Ahora bien, conviene enfatizar que la resolución del órgano competente de la que debe tenerse efectivo conocimiento no puede limitarse a (a´) declarar la ilicitud de los datos o de la lesión de derechos sino que deberá comportar (b´) la orden de retirada o de imposibilidad de acceso a los datos declarados ilícitos.

Como puede comprobarse, los requisitos legales para exigir responsabilidad jurídica (civil, penal o administrativa, según el art. 13 LSSI) al buscador Google por la indexación y divulgación de datos ilícitos parecen, a primera vista, diáfanos [23]

---

22 En idéntica dirección resulta bastante contundente la STJUE, de 23 de marzo de 2010 (C-236/08 y C-238/08), Google France vs Louis Vuitton, en la que su Gran Sala afirma: "las exenciones de responsabilidad establecidas en la Directiva 2000/31 sólo se aplican a aquellos casos en que la actividad del prestador de servicios de la sociedad de la información tiene naturaleza «meramente técnica, automática y pasiva», lo que implica que el prestador «no tiene conocimiento ni control de la información transmitida o almacenada». Por lo tanto, para comprobar si la responsabilidad del prestador del servicio de referenciación podría verse limitada con arreglo al artículo 14 de la Directiva 2000/31, es necesario examinar si el papel desempeñado por el prestador es neutro, es decir, si su comportamiento es meramente técnico, automático y pasivo, lo que implica que no tiene conocimiento ni control de la información que almacena... El órgano jurisdiccional nacional es el mejor situado para determinar el modo concreto en que se presta el servicio controvertido en los asuntos principales... el artículo 14 de la Directiva 2000/31 debe interpretarse en el sentido de que la norma que establece se aplica al prestador de un servicio de referenciación en Internet cuando no desempeñe un papel activo que pueda darle conocimiento o control de los datos almacenados. Si no desempeña un papel de este tipo, no puede considerarse responsable al prestador de los datos almacenados a petición del anunciante, a menos que, tras llegar a su conocimiento la ilicitud de estos datos o de las actividades del anunciante, no actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible".

23 A concretar su alcance ayuda, sin duda, la Sentencia del Tribunal Supremo 144/2013, de 4 de marzo, referida, precisamente, a un supuesto idéntico al que nos ocupa. La STS 144/2013 desestimó una demanda contra Google Inc por intromisión ilegítima en el derecho al honor por la difusión de informaciones que eran publicadas en diversas webs ("Aquí Hay Tomate", "PRNoticias" y "Lobby per la Independencia") y enlazadas por el buscador implicando al demandante en la trama de corrupción de Marbella conocida judicialmente como Operación Malaya.

V - La responsabilidad de google, compartida con el webmaster, como corolario del impacto de los buscadores de internet

La modalidad de asignación de responsabilidades a webs o buscadores de Internet respecto de las informaciones indexadas no resulta tan sencillo como *a priori* pudiera deducirse de las referida LSSI cuando se trata de verificar el cumplimiento de la legislación de protección de datos.

A falta de referencias específicas en la Directiva 95/46 y en la LOPD sobre cómo afectan a los buscadores de Internet los derechos y obligaciones derivados de la normativa de protección de datos, resulta imprescindible recurrir a los principios generales que deben presidir su aplicación.

El Dictamen 1/2008 del Art. 29 WP, atendiendo al principio de responsabilidad, diferencia entre responsabilidad principal (buscadores) y secundaria (proveedores de información) – y no siempre esta neta separación se cumple - pero siempre concurrentes.

Esto es, aunque en ocasiones parezca consolidada la interesada visión de que la responsabilidad en Internet resulta exclusivamente imputable a los proveedores de información mientras que los buscadores gozan de una suerte de impunidad/irresponsabilidad deriva de su supuesta neutralidad, nada más alejado de la realidad si atendemos al mejor criterio del Art. 29 WP que tiene encomendada esta función consultivo/interpretativa por la Directiva 95/46. Es verdad que, de entrada, una correcta aplicación del principio de proporcionalidad obliga a considerar que los motores de búsqueda actúan exclusivamente como intermediarios y, por lo tanto, no pueden ser considerados responsables principales del tratamiento o publicación en Internet de dichas informaciones. Máxime cuando los propietarios de las webs están en condiciones de evitar, mediante *robots.txt* y balizas *Noindex/No archive*, que los buscadores capturen dichas informaciones. Pero, ello no impide que la responsabilidad del buscador emerja *a posteriori* cuando se suscitan interrogantes sobre su licitud por vulnerar la normativa de protección de datos: « La responsabilidad formal, jurídica y práctica de los datos personales que incumbe al motor de búsqueda se limita generalmente a la posibilidad de retirar datos de sus servidores. Por lo que se refiere a la retirada de datos personales de su índice y de sus resultados de búsqueda, los motores de búsqueda tienen una responsabilidad suficiente para considerarse responsables del tratamiento (solos o conjuntamente con otros) en estos casos ».

Por lo tanto, en Google concurrirá una « responsabilidad suficiente » que le obligará a intervenir cuando se requiera la retirada de datos personales de su índice y de sus resultados de búsqueda en aplicación de la legislación de protección de datos. Inclusive los buscadores incurrirán en « entera responsabilidad » en muchos supuestos cuando no se limitan a actuar como simples intermediarios sino que (a') almacenan en sus servidores datos personales recabados de Internet, (b) u orientan la exploración, análisis e indexación mediante información identificable personalmente (como podría ocurrir con el reconocimiento facial).

En la sociedad de la información, los servicios prestados a través de Internet adquieren tal complejidad y generan tan heterogéneo impacto en la protección de datos que – lejos de admitir la impunidad absoluta - no resulta difícil imaginar una gradación en la responsabilidad de los

buscadores como la referida: « responsabilidad principal », « responsabilidad compartida », « responsabilidad entera »o « responsabilidad suficiente ».

Por ello, como recuerda el Dictamen 1/2008, la obligación de retirada de datos personales de los índices de búsquedas constituirá una responsabilidad de los buscadores de Internet en la medida en que la obligación de retirar o bloquear datos personales pueda depender de la legislación en materia de responsabilidad civil y de las normas en materia de responsabilidad del Estado miembro [24].

VI - El derecho de oposición como instrumento proporcionado/equilibrado para un ejercicio reactivo - ni preventivo ni censor - del derecho al olvido

Los derechos de protección de datos resultan receptivamente aplicables a la actividad de los motores de búsqueda. De nuevo, la apariencia de neutralidad generada por la actividad automatizada de intermediación de los buscadores supuestamente ajena a tratamiento alguno de datos personales no ha impedido que el Dictamen 1/2008 proclame la vigencia efectiva de los derechos de protección de datos a los buscadores. Cuestión bien distinta, habida cuenta de la diversidad de este fenómeno tecnológico, será la intensidad y viabilidad de ejercicio de estos derechos en función de las distintas actividades que generan los buscadores y de la distinta naturaleza de los sujetos concernidos. Diferente es la situación de los particulares según sean usuarios autenticados por los buscadores y con perfiles personales, usuarios no registrados o, incluso, terceros cuyos datos personales son alojados en webs y rastreados e indexados por los buscadores. Diferente será, también, la situación de las informaciones personales contenidas en perfiles personales registrados e historiales de búsqueda, en memorias cachés o en índices de los buscadores.

Explícitamente, el Dictamen 1/2008 refiere al derecho a solicitar la supresión de datos por los buscadores de Internet en los siguientes términos: 1) los buscadores deben respetar el derecho a suprimir datos - en particular, de los usuarios autentificados y de sus perfiles personales pero, también, a los no registrados -; 2) idéntico derecho se aplica a los datos de las memorias ocultas que los buscadores deben suprimir rápidamente cuando las informaciones resulten « incompletas u obsoletas », esto es, "una vez que estos datos no corresponden ya al contenido publicado en Internet por los responsables del tratamiento del sitio o sitios Internet que publican esta información"; 3) a los efectos anteriores, los buscadores deben actualizar las memorias ocultas mediante la actualización instantánea automática de la publicación original; 4) los editores de

---

24 Como ya hemos recordado anteriormente, el Dictamen 1/2008 menciona expresamente el caso español cuando señala que, "en algunos Estados miembros de la UE, las autoridades de protección de datos han regulado específicamente la obligación de los proveedores de motores de búsqueda de retirar datos de contenido del índice de búsqueda, sobre la base del derecho de oposición consagrado en el artículo 14 de la Directiva sobre protección de datos (95/46/CE) así como en la Directiva sobre el comercio electrónico (2000/31/CE). En virtud de estas legislaciones nacionales, los motores de búsqueda se ven obligados a seguir una política de notificación y retirada similar a la seguida por los proveedores de servicios de alojamiento, con el fin de evitar la responsabilidad".

webs deberían adoptar medidas para informar automáticamente a los buscadores de todas las solicitudes de supresión de datos que reciban.

Ahora bien, el derecho al olvido en Internet admite su ejercicio a través de dos instrumentos jurídicos que, aunque de apariencia similar y resultado idéntico, tienen un alcance bien diferente en Internet y, en particular, ante la actividad de sus buscadores: el "derecho de cancelación" y el « derecho de oposición ».

El derecho de cancelación previsto en el art. 16 LOPD dispone que el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de cancelación cuando el tratamiento de los datos no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos, dando lugar a su bloqueo durante los plazos previstos en la legislación o los derivados de las relaciones contractuales [25]. Como resulta evidente, proyectar genéricamente este derecho en Internet y, en particular, en la actividad de los motores de búsqueda resulta altamente conflictivo pues, la inexactitud, su carácter incompleto o la retirada o inexistencia de una autorización para el tratamiento de datos, comportaría una facultad habilitante para todo usuario que pondría ciertamente en cuestión la naturaleza misma y utilidad de los buscados como herramientas esenciales de la sociedad de la información.

Sin embargo, el *derecho de oposición* permite alcanzar idénticos objetivos (la supresión de datos personales indexados) pero por medios más acordes con el principio de proporcionalidad en la medida en que la supresión de datos requiere una ponderación individualizada de los motivos que pretenden justificarla y, por ende, no ampara una genérica habilitación de la supresión de información en Internet. Y ello es así por cuanto el art. 6.4 LOPD prevé que, en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que *una Ley no disponga lo contrario*, éste podrá oponerse a su tratamiento cuando existan *motivos fundados y legítimos relativos a una concreta situación personal* [26].

Por lo tanto, para la AEPD, el derecho de oposición contra las informaciones personales indexadas por los motores de búsqueda de Internet --como herramienta óptima para garantizar el derecho al olvido - se asentaría sobre las siguientes premisas legales y sociológicas:

---

25 Este precepto trae causa de la trasposición del art. 12 de la Directiva 95/46: "Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento... la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos".

26 El art. 14 de la Directiva 95/46 al trasponer el precepto anterior reza lo que sigue: "Los Estados miembros reconocerán al interesado el derecho a ... oponerse ... en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos". Y, a mayor abundamiento para clarificar el alcance de este derecho, la Directiva 95/46 establece en su Considerando 45: "cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias".

a) ausencia de filtrado preventivo de datos personales mediante instrumentos técnicos que pudieran semejar censura previa;

b) inexistencia de ley alguna que preceptúe el sometimiento de los individuos a que sus datos personales alojados en webs de Internet sean indexados y/o conservados temporalmente en las memorias ocultas de los motores de búsqueda;

c) alegación individualizada de motivos fundados y legítimos referidos a una situación personal concreta mediante un procedimiento reactivo;

d) falta de interés público de los datos personales publicados en Internet (ni personaje público ni hecho noticiable).

Como ha venido afirmando la AEPD, los extraordinarios efectos multiplicadores que hoy provocan en la difusión de datos personales tanto Internet, como instrumento de comunicación universal, como los motores de búsqueda que preservan su mantenimiento secular y global, obligan a habilitar instrumentos efectivos que preserven el derecho al olvido de forma proporcionada al impacto en la dignidad humana que puede generar la evolución de la sociedad de la información.

Habilitar un mecanismo jurídico que posibilite al individuo reaccionar frente a datos personales que se alojan en los índices de los buscadores, argumentando las circunstancias personales legítimas que amparan su supresión, no puede estimarse ni desnaturalizador de la indiscutible función social que desempeñan los buscadores de Internet ni siquiera desproporcionado.

VII- El derecho al olvido frente a los buscadores en el estado actual de desarrollo tecnológico: limitaciones técnicas

Todo lo anterior no impide, sin embargo, reconocer la debilidad del criterio resolutivo de la AEPD ante las dificultades técnicas que aparentemente plantea el cumplimiento de aquéllas de sus resoluciones que garantizan el derecho al olvido frente a los buscadores "instándoles a adoptar las medidas necesarias para retirar los datos personales de los índices de búsqueda e imposibilitar el acceso futuro a los mismos".

De entrada, retirar un determinado enlace de los índices de búsqueda por apreciar la concurrencia de motivos fundados y legítimos referidos a una concreta situación personal no debería plantear mayor dificultad técnica al motor de búsqueda – tras la tramitación de la correspondiente reclamación individual o de la resolución pertinente de la Autoridad de Protección de Datos competente -. La primera parte de los fallos resolutivos de la AEPD no plantea problema alguno adicional.

Por el contrario, la AEPD también exige, para garantizar el derecho al olvido, que los buscadores de Internet "adopten las medidas necesarias para imposibilitar el *acceso futuro* a los datos personales" contenidos en los enlaces de los índices contra los que se reconoce el derecho al olvido. Y es aquí donde las alegaciones de Google adquieren un valor no banalizable: sin la intervención del webmaster (mediante *robots.txt* o balizas *Noindex/No archive*) que limite el acceso

de los buscadores a su contenido, el buscador volverá a rastrear, almacenar, indexar y difundir los datos personales que fueron suprimidos del índice al admitirse el derecho de oposición.

Ante la alegación anterior, sólo parece caber la siguiente dicotomía: admitirla o no y, en su caso, derivar las correspondientes consecuencias jurídicas.

Lo cierto es que, a fecha de hoy, la supuesta imposibilidad técnica para evitar el acceso futuro de los buscadores a datos existentes en la Red (sin que el webmaster colabore) constituye un lugar común afirmado por la industria de Internet y aparentemente aceptado por la comunidad tecnológica. Sin embargo, este presupuesto ni ha sido nunca probado por quien estaría en condiciones de hacerlo (la propia industria de los buscadores de Internet) ni nada impide imaginar (a la vista de los extraordinarios progresos en los servicios de Internet) que la evolución tecnológica posibilite arbitrar mecanismos técnicos que permitan garantizar esta modalidad de derecho al olvido. Pero, si una norma o resolución administrativa obliga a "evitar el acceso futuro" y el buscador no poder probar su inviabilidad técnica, ¿cuáles serán los efectos jurídicos de dichos actos? ¿la imposibilidad del cumplimiento de la resolución devendrá en impunidad para el buscador seguirá siendo merecedor de reproche o sanción? [27]

Las cosas no son siempre necesariamente lo que parecen. La AEPD viene ordenando a Google "adoptar las medidas necesarias para imposibilitar el acceso futuro" a los datos retirados de los índices de búsqueda. Que de la retirada de los datos de los índices de búsqueda sólo es responsable Google, ninguna duda cabe. Pero "adoptar las medidas para evitar el acceso futuro a los datos" no significa necesaria y exclusivamente que Google - y sólo Google - deba evitar técnicamente el nuevo rastreo de los datos.

La AEPD ha optado por una fórmula resolutiva suficientemente abierta para adecuar la exigencia normativa al estado de desarrollo de la tecnología:

a) No deja mucho margen a la duda la obligada interpretación de que las resoluciones de la AEPD, cuando instan a Google a "adoptar las medidas necesarias para evitar el acceso futuro a datos personales", están *ordenándole* impedir directamente (sin colaboración del webmaster) que su buscador acceda a los referidos enlaces conforme a las posibilidades que ofrece el estado actual de desarrollo de la tecnología de los buscadores de Internet y, al tiempo, *invitándole* a perfeccionar la tecnología que permita tal actuación [28].

---

27 Resulta muy interesante el análisis que V. MAYER-SCHÖNBERGER realiza sobre la posibilidad ya existente de aplicar su propuesta de introducir fechas de caducidad de los datos a los resultdos de las consultas de los motores de búsqueda (Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, Oxford, 2009, págs. 179 y 180).

28 En definitiva, este criterio plasma la tesis mantenida por J. R. REIDEMBERG de que la solución a los problemas de jurisdicción y protección de derechos en Internet deberán proceder de la "innovación" en las tecnologías de la información: "the assertion of sovereign jurisdiction to protect citizens is likely to advance the fundamental public policy that the rule of law should be supreme to technological determinism. At the same time, the multiplicity of states with jurisdiction over Internet activities is likely to stimulate creativity and new Internet services such as more accurate and selective filtering technologies, stronger security zones and more robust, customized compliance capabilities" ("Technology and Internet Jurisdiction"..., pág. 1974).

b) Ahora bien, en tanto no existan instrumentos técnicos que permitan al buscador imposibilitar directamente (requiriendo, en consecuencia, la colaboración del webmaster) el rastreo de enlaces ya retirados con anterioridad del índice, "las medidas necesarias" a adoptar por Google se entenderán satisfechas con la tecnología que el buscador ya ofrece a los webmasters para limitar el acceso a los contenidos de las Webs.

Sin embargo, resulta difícil admitir la alegación de Google sobre la imposibilidad técnica de evitar el acceso futuro a resultados de búsqueda si tenemos en cuenta las previsiones contenidas en su *Política de Privacidad* referidas a *cómo eliminar contenido del sitio de otro usuario* [29], incluso, cuando el webmaster ni lo suprime ni evita su rastreo: "Eliminamos muy poco contenido de los resultados de las búsquedas de forma discrecional. Además del *spam*, solo tomamos medidas con ciertos tipos de datos personales (que especificamos a continuación) y con el "spam para adultos". Si un usuario nos lo solicita, eliminaremos información personal si creemos que puede perjudicarle de alguna forma en particular, como en casos de suplantación de identidad o fraude financiero. Entre este tipo de información se incluyen números de identificación nacional confidenciales, como el de la Seguridad Social, cuentas bancarias o tarjetas de crédito, así como imágenes de firmas. No se incluyen datos como la fecha de nacimiento, la dirección o el número de teléfono del usuario ... Para poder determinar si un tipo concreto de identificación se considera confidencial, aplicamos criterios como los siguientes: ¿Es un número de identificación emitido por el gobierno? ¿Es información privada o de dominio público? ¿Se puede utilizar para realizar determinadas transacciones financieras comunes? ¿Se puede utilizar para obtener más información sobre una persona? Aplicamos esta política de eliminación de contenido según las peculiaridades de cada caso. Normalmente no eliminamos esta información de sitios web gubernamentales oficiales, ya que en esos casos consideramos que la información es pública. A veces rechazamos solicitudes si creemos que alguien está intentando hacer un uso inadecuado de estas políticas para eliminar información de nuestros resultados. Eliminaremos cualquier página que contenga spam con contenido sexual explícito y el nombre completo de un usuario o de su negocio si recibimos una solicitud"[30].

De hecho, siguiendo el protocolo de Google para eliminar resultados de búsqueda existentes tanto en la web como en los índices, si el solicitante se ha puesto en contacto con el webmaster pero, por ejemplo, no ha recibido respuesta, Google admite al solicitante que "es posible que pueda ayudarle"[31] cuando los datos que se pretenden suprimir refieren a números de cuenta bancaria o de tarjeta de crédito, imagen de firma escrita a mano, contenido pornográfico que incluye un nombre completo, etc. Es decir, existe un explícito reconocimiento por Google de sus posibilidades técnicas de retirada de enlaces del índice del buscador.

VIII- Criterios específicos para los medios de comunicación online: ponderación entre el prevalente derecho a la información y la demanda legítima de olvido

29 http://support.google.com/webmasters/bin/answer.py?hl=es&answer=1663688

30 https://support.google.com/websearch/answer/2744324?

31https://support.google.com/websearch/troubleshooter/1209905#ts=1231445,2889054,2889099,2889064

Todo análisis jurídico del conflicto entre los derechos a la información y a la protección de datos deberá inevitablemente partir de la singular trascendencia que el primero tiene en las sociedades democráticas y de la necesidad de resolver dicho conflicto atendiendo a los siguientes fundamentos jurídicos:

1) No existe democracia sin elecciones libres ni éstas sin que los ciudadanos puedan formar libremente su opinión para lo que resulta indispensable el ejercicio de la libertad de expresión y el derecho a la información. Se trata de libertades que, más allá de su naturaleza como derecho subjetivo, tienen un valor institucional irrenunciable en el sistema democrático. Por ello, toda declaración constitucional de derechos viene proclamando durante los últimos siglos estas libertades en términos similares al vigente art. 20.1 de la Constitución Española: "Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción... d) A comunicar o recibir libremente información veraz por cualquier medio de difusión".

2) Ahora bien, en el sistema constitucional no existen derechos y libertades absolutos como el propia art. 20.4 CE evidencia palmariamente cuando proclama que los derechos anteriores tienen su límite en el respeto a los derechos constitucionalmente reconocidos "y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen". Es decir, existen derechos constitucionales especialmente *revalorizados* cuando se confrontan con las libertades informativas (por un lado, porque afectan a la esfera más personal del individuo y, por otro, porque su más impactante amenaza puede tener su origen en las libertades de información y expresión). Y a este grupo especialmente cualificado de derechos-límite debería entenderse incorporado el derecho a la protección de datos por implícita, pero inequívoca voluntad de la jurisprudencia constitucional que lo ha consagrado como derecho fundamental (STC292/2000). Sin embargo, este reciente reconocimiento constitucional no suplirá décadas y siglos de tradición en la protección del honor o de la intimidad y, en la práctica, su exigibilidad resultará notablemente más debilitada que en estos otros supuestos cuando entren en conflicto con las libertades informativas.

3) Resultando, a priori y en apariencia, equivalente su potencial constitucional, ¿cómo resolver los inevitables conflictos que se generarán cuando entren en conflicto las libertades informativas y los derechos fundamentales referidos (y, en particular, el de protección de datos)? Sin lugar a dudas, la jurisprudencia constitucional ha otorgado prevalencia a las libertades informativas [32]. Esto es, la información veraz sobre asuntos de interés público (que podrá venir dado tanto por la materia objeto de la información como por la identidad de quien la protagonice) sacrificará el derecho fundamental a proteger los datos personales de este último.

---

32 "Dada su función institucional, cuando se produzca una colisión de la libertad de información con el derecho a la intimidad y al honor aquélla goza, en general, de una posición preferente y las restricciones que de dicho conflicto puedan derivarse a la libertad de información deben interpretarse de tal modo que el contenido fundamental del derecho a la información no resulte, dada su jerarquía institucional, desnaturalizado ni incorrectamente relativizado. ... en esa confrontación de derechos, el de la libertad de información, como regla general, debe prevalecer siempre que la información transmitida sea veraz, y esté referida a asuntos públicos que son de interés general por las materias a que se refieren y por las personas que en ellos intervienen, contribuyendo, en consecuencia, a la formación de la opinión pública" (STC 171/1990)

4) Sin embargo, esta respuesta tradicional al conflicto tiene, hoy, tanto una plena e idéntica predicabilidad en la actividad de los medios de comunicación vigentes como, al tiempo, un impacto sin precedentes en la moderna sociedad de la información y del conocimiento que genera no poca confusión sobre cómo resolver estos conflictos ante los medios de comunicación online [33] y, singularmente, ante la existencia de servicios de Internet, como los buscadores, que multiplican extraordinariamente los efectos divulgativos de cualquier información. Si el constituyente español ya mostró su preocupación por los efectos del uso de la informática en el acervo de derechos y libertades (art. 18.4 CE), intuyendo los riesgos de una tecnología cuya actual trascendencia resultaba inimaginable por aquel entonces, parece incontestable que la actualización hermenéutica de este mandato constitucional conforme a la realidad social actual obliga inexorablemente a "revalorizar" el derecho a la protección de datos como instituto de garantía especifico e idóneo (STC 292/2000) en la sociedad de la información articulada en torno a Internet.

5) Así las cosas, la Resolución de la AEPD 266/2007 ya avanzó un criterio básico – pero, como veremos, no suficiente - para resolver el conflicto entre protección de datos en Internet y libertades informativas [34]. Ahora bien, si el límite al derecho al olvido en Internet reside en que los datos refieran a una persona física que protagoniza un asunto de interés público, ¿cuándo hay que entender cumplido este requisito? En otras palabras, ¿un hecho (y los datos personales que lo acompañan) deviene en información (veraz y de interés social) sólo si acredita esas condiciones antes de ser publicado en un medio de comunicación o, por el hecho de su publicación ya le resultan predicables esas notas distintivas? No es éste un interrogante baladí si tenemos en cuenta que la Constitución ampara la libertad de información "por cualquier medio de difusión (art. 20.1 d) CE) – y, desde luego Internet es su más paradigmática expresión – y que la jurisprudencia constitucional proscribe privilegio o "derecho fundamental reforzado" en favor de periodistas o medios de comunicación respecto de los ciudadanos en tanto titulares todos de las libertades de expresión e información (STC 225/2002). Por ello, resultará imprescindible un juicio en la publicación de datos personales en Internet que pondere la gradación del interés social o relevancia pública de una información personal en función del entorno divulgativo en el que se transmite: webs, buscadores, medios de comunicación online, etc.

---

33 UNa específica manifestación de esta realidad conflictual, en RALLO, A. y MARTINEZ, R.: "Data Protection, Social Networks, and Online Mass Media", European Data Protection: Coming of Age, Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet Editors, ed. Springer, London-New York, 2013, págs. 407 a 430.

34 "Ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la Red sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación inconsentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar basilar del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal".

6) Conviene advertir que la Directiva 95/46 de protección de datos atribuye a los Estados la potestad de establecer exenciones y excepciones a las normas de protección de datos en la medida en que resulten necesarias para conciliar el derecho a la intimidad y la libertad de expresión en el tratamiento de datos personales con fines exclusivamente periodísticos (art. 9). Además, su Considerando 37 insiste en la necesidad de prever excepciones o restricciones siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión "y, en particular, la libertad de recibir o comunicar informaciones", tal y como se garantiza en el artículo 10 CEDH". El mandato por lo tanto es claro: no sólo ponderar a la búsqueda del equilibrio –y, en su defecto, sacrificar el derecho a la protección de datos en beneficio del preferente derecho a la información- sino "conciliar" ambos derechos en la medida de lo posible o, cuanto menos, minimizar el sacrificio de uno respecto del otro.

7) Ante el reto de lograr tal conciliación sin sacrificar la libertad de información, la AEPD constata, en primer lugar, que "el desarrollo de internet y la implantación generalizada de los motores de búsqueda suponen una actualización y divulgación exponencial y permanente de la información" y, por ello, recomienda (entre los numerosos casos, en Resolución 2010/2012) a todos los medios de comunicación online partes en litigios sobre el derecho al olvido seguir las siguientes técnicas y procedimiento: 1) valorar la necesidad de que su actuación se dirija a conciliar, en mayor medida, el derecho a la libertad de información con la aplicación de los principios de protección de datos personales; 2) ponderar escrupulosamente la relevancia pública de la identidad de las personas afectadas por el hecho noticiable; 3) en el caso de que la identidad de las personas no aporte información adicional, evitar la identificación mediante la supresión del nombre e, en su caso, de las iniciales y cualquier referencia suplementaria de la que pueda deducirse la identificación; 4) reflexionar sobre la trascendencia que tiene mantener de manera permanente una absoluta accesibilidad de los datos contenidos en noticias cuya relevancia informativa, probablemente, es inexistente en la actualidad; 5) usar medidas informáticas - por ejemplo, los ficheros "robots.txt" - para evitar desde la web la indexación de noticias con datos personales por los motores de búsqueda de internet y, con ello, impedir su divulgación indiscriminada, permanente y, en su caso, lesiva – pero sin alterar fondos documentales o hemerotecas-.

7) Sin embargo, los motores de búsqueda de Internet no gozan de amparo legal específico para disponer de la información personal e incorporarla a sus índices de búsqueda o conservarla temporalmente en la memoria "caché". Esto es, la libertad de información sería predicable sólo de quienes publican noticias con datos personales pero no de los buscadores de Internet que estarían obligados, en su caso, a evitar la indexación de los mismos e impedir futuras captaciones.

8) Con todo, lejos de habilitarse una suerte de censura [35] preventiva o reactiva de carácter general o una pretensión de olvido genérico, los límites anteriores a la actividad informativa de los

35 Y, como puede observarse, los criterios anteriores cumplen plenamente los parámetros propuestos por F. LA RUE para considerar legítima una restricción de contenidos en Internet: "As with offline content, when a restriction is imposed as an exceptional measure on online content, it must pass a three-part, cumulative test: (1) it must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); (2) it must

medios de comunicación online o a la captación por los buscadores de Internet sólo podrían sustentarse en la existencia de motivos fundados y legítimos referidos a una situación personal que ampararan el ejercicio del derecho de oposición previsto en el art. 6.4 LOPD. Y, en particular, la AEPD ha estimado que dichos motivos podrán consistir: 1) en la inexactitud de las informaciones; 2) o en la pérdida del interés informativo de la noticia derivada de un significativo paso del tiempo que la haya tornado en obsoleta.

---

pursue one of the purposes set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights , namely: (i) to protect the rights or reputations
of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and (3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality). In addition, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory. There should also be adequate safeguards against abuse,including the possibility of challenge and remedy against its abusive application" (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Asamblea General de Naciones Unidas, 16 mayo 2011, pág. 19).

QUATRIEME PARTIE

Le droit à l'oubli entre théorie et pratique

CHAPITRE 1

Droit à l'oubli numérique : quel alignement entre chartes et pratique ?[1]

1. Données personnelles et droit à l'oubli numérique. Aujourd'hui, sont essentiellement évoquées les données personnelles, à savoir le caractère privé de celles-ci et le problème lié à leur divulgation. Dans cette quête de préservation de l'intimité et de la confidentialité des données relatives à une personne, le droit à l'oubli numérique semble proposer un moyen de lutte adéquat. En effet, la confidentialité de la personne peut être certes promue *a priori*, avec une absence de divulgation des données liée à leur caractère privé, mais lorsque cela n'est pas possible, ou que cette étape a tout simplement été dépassée, le droit à l'oubli numérique peut intervenir *a posteriori*, comme remède.

2. Définition du droit à l'oubli numérique. Seulement, le droit à l'oubli numérique, tel qu'il peut être entendu comme un droit pour les personnes de faire valoir l'anonymisation de données privées les concernant[2], soulève des interrogations relatives à son applicabilité concrète. En effet, en deçà du lien direct qui peut exister entre le législateur et l'individu, le droit à l'oubli numérique a vocation à être appliqué par l'intermédiaire de personnes morales, qu'elles soient de droit public ou de droit privé. Cependant, il n'est actuellement nullement imposé « en tant que tel »[3] au titre du droit positif français. Il convient à ce titre de noter que le droit à l'oubli numérique est régulièrement confondu avec le droit à la protection de la vie privée[4], et que cet élément tend à se refléter en pratique au regard de l'étude des chartes et des pratiques mises en œuvre dans l'ensemble des structures privées et publiques.

---

1 par Sophie Guicherd, docteur en droit, faculté de droit de Grenoble ; Marie-Laurence Caron –Fasan, professeur à l'institut d'Administration des entreprises de Grenoble et Nicolas Lesca, professeur à l'université Lyon1

2 Jusqu'à « se muer en droit d'opposition »: v. A. Lepage, « "Droit à l'oubli" : sanction de la CNIL », Comm. com. électr. n°12, déc. 2011, comm. 115 sous CNIL, délib. n° 2011-238 de la formation restreinte, 12 juill. 2011 : www.cnil.fr.

3 A. Lepage, « Où il est de nouveau question du "droit à l'oubli" sur l'Internet », Comm. com. électr. n°5, mai 2012, comm. 54 sous TGI Paris, réf. 15 févr. 2012, Diana Z. c. Google, [www.legalis.net]; TGI Paris, 14 janv. 2013, 17ème ch., RG n° 11/03875 : « le demandeur encore détenu au titre de cette condamnation ne saurait invoquer un droit à l'oubli qui n'est consacré par aucun texte ».

4 CNIL, formation restreinte, délib. n°2011-238, 12 juill. 2011, [www.cnil.fr]; A. Favreau, « La délibération de la CNIL du 12 juillet 2011, une pierre dans l'édifice d'un droit à l'oubli », RLDC n° 92, avr. 2012, p. 53 et s. V. en ce sens aussi TGI Paris, 14 janv. 2013, 17ème ch., RG n° 11/03875 où les juges traitent de la question d'un éventuel droit à l'oubli dans le cadre du respect de la vie privée du demandeur.

3. Intérêt du sujet. L'effectivité du droit à l'oubli numérique est intimement liée aux textes propres à être appliqués au sein même des structures que recouvrent ces personnes morales. C'est ainsi que l'étude des chartes mais aussi des pratiques au sein d'un échantillon d'entreprises privée et publiques s'est imposée afin d'apprécier l'effectivité de ce droit. Dans ce cadre, les chartes, comme « **instrument[s] de** "soft law" »[5], correspondent juridiquement à un « document fondamental ; acte inaugural formant la base immuable de rapports juridiques durables »[6] entre les parties, autrement-dit en l'occurrence, entre la personne morale et l'ensemble des personnes physiques qui interagissent avec elle.

L'intérêt qui ressort de la démarche d'étude des chartes et des pratiques est avant tout de percevoir les implications pratiques du droit à l'oubli numérique, et même, de sonder si celui-ci existe véritablement. En effet, après avoir étudié un certain nombre de chartes et de pratiques, nous constatons que le droit à l'oubli numérique existe parfois, mais qu'il demeure encore bien sujet à confusion. D'une part, il n'est pas toujours présent au sein des chartes, certainement parce qu'il reste encore méconnu, et mal identifié ; d'autre part, il fait l'objet d'une confusion réelle avec la protection des données personnelles en général telle qu'elle est imposée par le droit existant[7], et qui concerne alors avant tout les méthodes et les possibilités de diffusion des données à caractère personnel[8].

Ainsi, l'objectif de l'étude est d'identifier si le droit à l'oubli numérique est traité dans les entreprises, en analysant d'une part leurs chartes, et en questionnant d'autre part leurs pratiques au travers d'entretiens.

4. Constat général qui ressort de l'étude. En réalité, il ressort de l'étude des chartes et des pratiques un attachement plus vigoureux aux mesures préventives relatives aux données personnelles, qui peut s'expliquer notamment parce que la loi l'impose explicitement. En effet, la majeure partie des dispositions rédigées dans les chartes concerne la protection des données par la maîtrise de leur divulgation, que celle-ci soit imposée à l'utilisateur[9] et/ou qu'elle soit prise en charge par l'entreprise concernée. Cependant, la protection des données par le biais du développement des moyens de prévention ne s'avère pas forcément suffisante. Elle émerge du postulat de la maîtrise de la divulgation, et ne permet pas de prendre en compte les données qui échappent à cette maîtrise. Elle ne résout pas non plus le cas des données qui ont volontairement fait l'objet d'une divulgation, mais qui peuvent être soumises à un droit à l'oubli, parce que la légitimité de leur divulgation a disparu avec le temps ou les évènements postérieurs à celle-ci. En effet, il existe à ce titre des données qui sont nécessairement divulguées, au titre par exemple de l'emploi de la personne, de son activité, ou encore de la loi, notamment en cas de faits pénalement répréhensibles ; mais il existe aussi des données qui échappent à la vigilance nécessaire à leur préservation dans la sphère intime, lorsqu'elles font l'objet de stockage sur un serveur mal sécurisé par exemple. Ainsi, il apparaissait nécessaire dans le cadre de cette étude de

---

5 C. Thiérache, « Le droit à l'oubli numérique : un essai qui reste à transformer », RLDI 2011, 67.

6 G. Cornu, Association Henri Capitant, Vocabulaire juridique, Puf, 7ème édition, p.147.

7 V. en ce sens notamment, loi n° 78-17 du 6 janvier 1978, art. 38, modifié par la loi n°2004-801 du 6 août 2004

8 A. Caprioli, « Loi du 6 août 2004. Commerce à distance sur Internet et protection des données à caractère personnel », Comm. com. électr. n°2, févr. 2005, étude 7.

9 L'utilisateur doit être entendu comme étant la personne qui fait usage du dispositif informatique et qui est susceptible d'y stocker des données à caractère personnel.

mener des entretiens avec les personnes responsables de la gestion des données informatiques au sein de diverses entreprises privées comme publiques.
Ces écueils, réels, ne peuvent pas être traités par des moyens préventifs, mais seulement curatifs. C'est pourquoi la raison d'être du droit à l'oubli numérique n'est ici guère contestée.

5. Présentation du plan. Cependant, le droit à l'oubli numérique est mis en œuvre de manière très inégale selon les entreprises. C'est pourquoi il apparaît nécessaire de mettre en évidence les clauses pertinentes qui ressortent de l'étude des chartes analysées (1), avant d'appréhender la mise en pratique du droit à l'oubli numérique au sein de diverses entreprises privées et publiques grâce aux entretiens menés avec leurs Correspondants Informatique et Libertés (2). Ces deux axes d'étude permettent ainsi d'adopter une vision d'ensemble de la mise en œuvre du droit à l'oubli numérique dans les entreprises privées et publiques, et d'en extraire les principales problématiques propres à mettre en cause son effectivité (3).

6. Méthodologie de l'étude. Deux types de données sont étudiés :

- les chartes relatives à l'usage des systèmes d'information des entreprises privées et publiques pour étudier la manière dont le droit à l'oubli numérique est traité dans ces textes ;
- des entretiens auprès des Correspondants Informatique et Liberté (CIL) de ces mêmes entreprises lorsqu'ils nous ont donné leur accord pour étudier la manière dont le droit à l'oubli numérique est mis en œuvre et les difficultés que cela soulève en pratique.

4 secteurs étaient plus précisément ciblés : les sociétés de services en ingénierie informatique (SSII), les collectivités publiques, les organismes de santé et les universités.

Sur les 29 entreprises contactées (cf. tableau 1) :

- 14 ont accepté de transmettre leur charte,
- 14 ont refusé de nous transmettre leur charte, en invoquant le plus souvent leur caractère confidentiel, et dans une moindre mesure parce qu'elles n'en avaient pas (encore).
- 5 ont accepté de s'entretenir avec nous, dont une qui n'avait pas (encore) de charte.

Entreprises contactées			Données	
Secteur	Type	Refus	Charte	Entretien
Privé	SSII	7	1	2
	Autres	2	-	-
Public	Universités	-	11	1
	Santé	2	1	1
	Autres	3	1	1
Totaux		14	14	5

Tableau 1 – Collecte de données

Les chartes et les entretiens ont été analysés séparément en utilisant la même grille de codage thématique pour en extraire des parties et les organiser en trois catégories principales (cf. tableau 2) :

- qu'est-ce que le droit à l'oubli numérique et quelles sont ses finalités (DTO) ?
- sur quels traitements des données personnelles porte le droit à l'oubli numérique (DON) ?
- quels sont les moyens et les limites de la mise en œuvre du droit à l'oubli numérique (MOE) ?

Codage	Thèmes et sous-thèmes
DTO	**Définitions et finalités du droit à l'oubli numérique**
- DTOdef	Définition
- DTOfinal	Finalités
DON	**Traitement des données**
- DONstock	Stocker les données
- DONsupr	Détruire les données
- DONanony	Anonymiser les données
- DONmaj	Mettre à jour les données
- DONacces	Accéder aux données
- DONsecur	Sécuriser les données
- DONtrans	Transférer les données
MOE	**Mise en œuvre du droit à l'oubli numérique**
- MOEtech	Mise en œuvre technique
- MOElegal	Mise en œuvre légale
- MOEprat	Mis en œuvre pratique (communication, formation, sensibilisation)

Tableau 2 – Grille de codage thématique des chartes et des entretiens

Section 1- Le traitement du droit à l'oubli numérique dans les chartes

I - Des principes généraux déclarés

Des principes généraux sont régulièrement déclarés par les entreprises ayant mis en place les chartes. Ils évoquent les problèmes relatifs à la gestion des données qui doit faire l'objet d'une véritable attention de la part des entreprises privées et publiques, et des utilisateurs, qui sont à cet égard, effectivement aussi largement responsabilisés dans leurs actes.

Les chartes s'efforcent à ce titre de rappeler les principes prévus par la loi Informatique et Libertés[10] sur la protection des données à caractère personnel (Public_Autre_1). Certaines se

10 Loi 78-17 du 6 janvier 1978, modifiée à de nombreuses reprises.

proposent même d'accompagner l'utilisateur dans une démarche de gestion éclairée de ses données (Public_Univ_1).

II- Des dispositions essentiellement orientées sur la protection des données à caractère personnel

Il est à souligner qu'à l'issue de l'étude des chartes, il ressort une orientation particulièrement fixée sur la protection des données privées des personnes concernées. Certaines chartes mettent lourdement l'accent sur cet aspect constituant pour l'entreprise une priorité (Public_Autre_1, Public_Univ_1, Public_Univ_2).

Régulièrement, la responsabilité de l'entreprise est reconnue, en ce qu'elle doit garantir la sécurité et la confidentialité des données (Public_Autre_2 : « L'administrateur est susceptible d'accéder à des informations dont le contenu, personnel ou confidentiel, est couvert par le secret des correspondances ou relève de la vie privée. De ce fait, il est tenu au secret professionnel et à l'obligation de confidentialité », Public_Autre_1 : on observe à ce titre parfois une obligation de moyens : « L'université met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs »), Public_Santé_1 : « le responsable du fichier doit s'engager à prendre toute précaution utile afin de permettre la sécurité des informations », à travers notamment la responsabilité de l'administrateur.

Des moyens sont alors mis en œuvre pour assurer la sécurité et la confidentialité des données :

- D'une part, des moyens techniques :
- Principalement par la sécurisation des accès aux données avec l'emploi de codes et mots de passe : Privé_SSII_1 (pour l'ensemble des données au sein de l'entreprise) : « Le contrôle d'accès aux moyens informatiques du groupe est lié à la possession d'un identifiant nominatif et unique ainsi que d'un mot de passe. Le mot de passe doit respecter les règles de sécurité en vigueur (complexité, longueur, cycle de vie). Cet identifiant et mot de passe sont strictement personnels et ne doivent en aucun cas être communiqués, prêtés, écrits ou divulgués pour quelque raison que ce soit. L'utilisateur ne doit pas usurper, emprunter ou obtenir l'identifiant et mot de passe d'autres utilisateurs. Il doit protéger l'accès à son poste de travail en verrouillant sa session lorsqu'il quitte son poste de travail » ; « Afin de se prémunir d'un usage frauduleux du système d'information, les utilisateurs possèdent un identifiant et un mot de passe personnels » ; Public_Autre_1 : « L'utilisateur se voit attribuer un identifiant ayant un caractère confidentiel » ; Public_Univ_3 : « Le droit d'accès à un système informatique est soumis à autorisation ; il est personnel et incessible, et cesse lorsque les raisons de cet accès disparaissent » ; « Cet accès est possible par l'intermédiaire d'un compte utilisateur, mais aussi, directement à partir d'un micro-ordinateur (et dans ce cas, avec certaines restrictions) » ; « chaque utilisateur a le devoir de choisir un mot de passe » ; Public_Univ_4 : « Chaque utilisateur se voit attribuer, par l'autorité d'enregistrement, un identifiant et choisit un mot de passe qui lui permettra de se connecter aux ressources informatiques et/ou services internet. Ces autorisations sont personnelles et ne peuvent en aucun cas être cédées ou communiquées ».
- Ou encore des logiciels de protection : Privé_SSII_1 : « La configuration des logiciels de protection contre les virus, les logiciels espions, les intrusions et autres attaques ne doit pas être modifiée. Toute contamination devra être immédiatement signalée à la direction

des systèmes d'information du client et du groupe par le biais du helpdesk » ; Public_Santé_1 : « Le réseau interne est sécurisé. Toute interconnexion avec des réseaux extérieurs et en particulier internet, doit passer impérativement par le dispositif de pont et de firewall qui a été conçu pour contrer d'éventuelles intrusions ».

- Ou des contrôles réguliers par la mise en place d'audits : Privé_SSII_1 : « Pour assurer le bon fonctionnement des moyens informatiques du groupe, il est procédé à des audits, dans le respect de la confidentialité et de la vie privée des utilisateurs ».
- Et plus généralement, par le contrôle de l'utilisation d'internet : Privé_SSII_1 : « L'entreprise se réserve le droit, d'effectuer des contrôles sur l'utilisation d'internet à des fins statistiques de traçabilité, d'optimisation, de sécurité ou de détection d'intrusion et d'utilisation contraire à l'ordre public et aux bonnes mœurs » ; Public_Autre_1 : « Les connexions internet font l'objet de supervisions, de vérifications et d'audits réguliers dans le respect global des règles législatives, réglementaires et jurisprudentielles » ; Public_Santé_1 : « Le bénéficiaire des services internet est informé que, du poste sur lequel il se connecte, il peut accéder au réseau extérieur mais aussi au réseau interne de l'hôpital sur lequel ils sont connectés des services administratifs et médicaux, et qu'une utilisation négligente ou malveillante de ses droits pourrait donner accès à ces gisements d'information ».
- D'autre part, par des moyens humains, par la détermination de personnes spécifiquement dédiées à cette tâche :
- À travers la mission du CIL, interagissant avec les démarches relatives à la gestion des données. Public_Univ_2 : le CIL « est obligatoirement consulté préalablement à la création, modification même mineure, transformation, transfert de données et interconnexion concernant tout traitement informatisé d'informations nominatives mis en œuvre ou hébergé dans l'un quelconque des services de l'université, de ses composantes et de ses laboratoires ou du Service Commun Informatique. Il veille à la protection des droits des usagers et des personnes concernées par de tels traitements ».
- Mais aussi d'autres types de responsables : Public_Univ_5 : « Toute publication de pages d'information sur les sites internet ou intranet de l'université doit être validée par un responsable de site ou responsable de publication ».

Cependant, il arrive que certaines entreprises écartent leur responsabilité à ce titre et par exemple les entreprises publiques. Quoi qu'il en soit, l'accent est largement mis sur la responsabilisation de l'utilisateur :

- Privé_SSII_1 : « Chaque salarié est responsable de l'usage des moyens informatiques et des informations mis à sa disposition ».
- Public_Univ_6 : « L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède ».
- Public_Univ_7 : « Tout utilisateur est responsable de son utilisation des ressources informatiques, il s'engage à ne pas effectuer des opérations contraires à la loi pouvant nuire au fonctionnement du réseau, à l'intégrité de l'outil informatique, et aux relations internes et externes de l'établissement. Il doit en particulier utiliser le réseau de façon rationnelle en évitant les applications consommatrices de ressources sur les liaisons

externes. La sécurité est l'affaire de tous, chaque utilisateur de l'informatique et du réseau d'établissement doit y contribuer et mettre en application les règles de bon sens et les recommandations fournies par les administrateurs et les responsables de l'outil informatique ».

- Public_Autre_2 : « Afin d'assurer la confidentialité des données de l'organisme et de celles dont il se trouve dépositaire, l'utilisateur s'engage à appliquer les recommandations de sécurité ».

Il existe par ailleurs des disparités de protection à ce titre, dans la mesure où les chartes ne sont pas positionnées de la même façon à l'égard de la présomption du caractère personnel ou professionnel des données. En effet, la plupart d'entre elles sont orientées sur la définition d'une présomption du caractère professionnel des données, mais d'autres, sont au contraire axées en faveur de l'utilisateur à cet égard :

- Présomption du caractère professionnel des données (informations en général et/ou messages électroniques) :

- Privé_SSII_1 : « L'utilisateur qui souhaite utiliser, à des fins privées, les moyens informatiques mis à sa disposition est tenu de l'indiquer clairement et explicitement par l'utilisation du terme "personnel" ou " privé". Cette mention doit obligatoirement apparaître dans le nom des fichiers ou répertoires ou dans le sujet des messages concernés. Toutes les informations qui ne sont pas clairement identifiées comme "personnel" ou "privé", sont considérées comme des informations professionnelles ».

- Public_Univ_2 : « tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données ».

- Public_Univ_4 : « Toute information est professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage éventuel de ses données à caractère privé dans des répertoires ou des dossiers explicitement prévue à cet effet et intitulés " privé" » ; « Tout message sera réputé professionnel sauf s'il comporte la mention particulière "privé", explicitée dans son objet indiquant son caractère privé ou s'il est stocké dans un espace privé de données intitulé "privé". L'utilisateur ne doit pas transformer de message de nature professionnelle en correspondance privée ».

- Public_Univ_6 : « Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données ».

- Public_Univ_8 : « Toute information est réputée liée à l'activité de service public à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée ».

- Public_Autre_2 : « tous les courriels dont le caractère personnel est explicitement exprimé (objet ou dossier "personnel") sont considérés comme "privés". L'employeur ne peut donc prendre connaissance de leur contenu ».

- Présomption du caractère personnel des données :

- Public_Univ_3 : « Les fichiers appartenant à un utilisateur sont considérés comme privés, qu'ils soient ou non accessibles par les autres utilisateurs. La possibilité de lire un fichier n'implique pas la permission de lire ce fichier. Les fichiers qui appartiennent à un individu sont considérés comme une propriété privée ».
- Public_Univ_9 : « Les données contenues dans des fichiers ou transmises sur les réseaux par des utilisateurs ou des administrateurs doivent être considérées comme privées, qu'elles soient ou non accessibles par les autres utilisateurs ».

III- Le droit à l'oubli numérique indirectement et directement consacré

Le droit à l'oubli numérique est malgré tout présent dans les chartes, de manière indirecte, mais aussi directe, au regard notamment de la gestion de la conservation et de la destruction des données.
Ainsi, de manière indirecte, il est possible d'en trouver une manifestation par la confidentialité propre à l'interdiction de toute divulgation lorsque celles-ci sont accessibles dans un cadre particulier. Par conséquent, il existe des interdictions formelles d'accès aux données sauf autorisation spécifique, mais surtout, lors du traitement des données, les administrateurs n'ont pas l'autorisation de communiquer ces données sauf en cas de risque particulier qui serait alors encouru :

- *Privé_SSII_1 : interdiction de :* « l'accès aux données personnelles d'une tierce personne sans l'autorisation de celle-ci » *et* « Les administrateurs sont tenus à une obligation de discrétion et de confidentialité dans le cadre de leur fonctions. Ainsi, ils ne peuvent exploiter les informations et données professionnelles et personnelles relatives à un utilisateur, qu'à des fins visant à garantir le bon fonctionnement et la sécurité des moyens informatiques du groupe. Dans le cadre des procédures de contrôle prévues à l'article 6 de la présente charte : l'administrateur peut communiquer à l'employeur toutes informations et données professionnelles relatives à un utilisateur; l'administrateur ne peut pas communiquer des informations et données identifiées "personnel" ou "privé", sauf risque ou évènement particulier ».

- *Public_Univ_2 :* « L'accès étendu dont dispose une administrateur ne doit pas contrevenir au respect de la vie privée des usagers. Les administrateurs sont ainsi soumis au secret professionnel ».

- *Public_Univ_4 :* « Les personnels en charge des opérations de contrôle, de maintenance ou de gestion technique sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction ».

- *Public_Univ_6 :* « Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur ».

Au-delà de ces aspects, entre la protection du caractère privé et l'assise d'un futur droit à l'oubli numérique, il existe dans les chartes un devoir d'information à l'égard des utilisateurs sur le traitement des données :

- *Privé_SSII_1 :* « Les utilisateurs sont informés de ce que la messagerie électronique nominative ou partagée peut faire l'objet d'un contrôle en cas de litige interne ou externe sur l'utilisation qui en est faite » *et* « Les utilisateurs sont informés de ce que l'usage qu'ils font des moyens informatiques et de communication mis à leur disposition peut donner lieu à enregistrement et conservation de données qui les concernent ».

- *Public_Univ_2 :* « Les ressources informatiques de l'université, administrées par les administrateurs, peuvent contenir ou traiter des données privées d'utilisateurs. Les administrateurs doivent veiller à protéger ces données, et à communiquer aux utilisateurs toute information utile sur les mesures ou évènements les concernant », « L'utilisateur est informé que les traces enregistrées ne retiennent pas le contenu même des données échangées mais seulement les données de connexion ».

- *Public_Santé_1 :* « Les patients doivent être informés que des données nominatives les concernant font l'objet d'un enregistrement et qu'ils ont des droits : droit d'opposition : ce droit peut néanmoins être retreint dans certains cas, notamment lorsque les traitements informatiques sont opérées pour le compte de l'état ou les collectivités territoriales, et sous certaines conditions ; droit d'accès indirect par l'intermédiaire d'un médecin désigné par l'intéressé ; droit de rectification : le titulaire du droit d'accès peut exiger que soient rectifiés, complétées, clarifiées, mises à jour ou effacées, les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte ou l'utilisation, la communication sont interdites ».

Par ailleurs, est très nettement consacré dans certaines chartes un droit de modification ou de suppression des données concernant les utilisateurs, conformément en réalité aux dispositions de la loi Informatique et Libertés :

- *Public_Univ_2 :* « chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des ressources informatiques ».

- *Public_Univ_6 :* « chaque utilisateur dispose d'un droit d'accès, de rectification, le cas échéant d'opposition, relatif aux données le concernant, y compris les données portant sur l'utilisation des systèmes d'information ».

Enfin, en ce qui concerne la destruction des données :

Elle est envisagée dans certaines chartes comme un devoir de l'utilisateur à son départ de la structure en question :

- Privé_SSII_1 : « Toutes les données personnelles et les données clients doivent avoir été effacées par l'utilisateur avant la restitution du matériel ».

- Public_Univ_4 : « Il appartient à l'utilisateur, lors de son départ définitif de l'établissement, de détruire toutes données à caractère privé ».

- Public_Univ_5 : « Les serveurs de messagerie effectuent la sauvegarde temporaire des boîtes à lettres en prévention des erreurs de manipulation des utilisateurs et des pannes des équipements. Cette sauvegarde ne garantit pas le recouvrement de l'ensemble des messages reçus. Les utilisateurs devront pouvoir effectuer la restauration ou la destruction des messages sauvegardés ».

- Public_Univ_6 : « L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'établissement ne pouvant être engagée quant à la conservation de cet espace ».

Elle est aussi envisagée dans certaines chartes comme un devoir prévu pour l'administrateur, qu'il œuvre pour une entreprise privée ou publique, avec la prévision d'un délai maximal de conservation :

- Privé_SSII_1 : « Le répertoire "privé" ou "personnel" d'un utilisateur quittant la société, s'il n'a pas été détruit par ce dernier, sera supprimé sans copie, ni prise de connaissance préalable du contenu par la société sous réserve d'un contrôle réalisé dans les conditions prévues à l'article 6 ci-après. Le départ d'un utilisateur entraîne la fermeture immédiate des accès à sa boîte aux lettres et la suppression de la boite aux lettres dans un délai d'un mois, sauf décision contraire de l'autorité hiérarchique de l'utilisateur et sans toutefois pouvoir dépasser un délai de conservation de six mois. Durant cette période de conservation, la société se réserve le droit d'accéder aux messages professionnels reçus dans la boîte aux lettres. Il est de la responsabilité de l'utilisateur de faire suivre ses messages à caractère personnel en communiquant sa nouvelle adresse à ses interlocuteurs » et « Les utilisateurs sont informés de ce que l'usage qu'ils font des moyens informatiques et de communication mis à leur disposition peut donner lieu à enregistrement et conservation de données qui les concernent. À cet égard, il est précisé que : les connexions internet sont enregistrées et archivées par la société pendant une durée de 6 mois ; tout message électronique reçu ou envoyé peut être conservé par l'Entreprise pendant une durée maximale de 6 mois, à compter de la date d'émission ou de réception. Au-delà, toutes les données sont détruites ».

- Public_Univ_2 : « La durée de conservation des traces est de 1 an maximum. L'université s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme ».

- Public_Autre_1 : « Le responsable de traitement est tenu de conserver les 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 ».

Section 2- Le traitement du droit à l'oubli numérique en pratique

7. Une terminologie inexistante. L'expression « Droit à l'oubli numérique » n'existe pas dans les entreprises interrogées. Cette expression qui n'existe pas non plus dans la loi Informatique et Libertés, n'est ni utilisée dans les chartes ni par les personnes dans le cadre de leur activité.

- *Privé_SSII_1 :* « Alors, il n'est pas traité en tant que finalité ou... Enfin, il n'est pas abordé de manière indépendante. Les éléments dans lequel on peut le retrouver sont uniquement le respect des recommandations de la CNIL relatives à la conservation de données à caractère personnel après un certain délai ».
- *Public_Univ_6 :* « Il n'y a pas de phrase ou d'expression qui dise « droit à l'oubli ».

Le terme est compris et ne suscite pas d'interrogation : il ne plonge pas les personnes interrogées dans la perplexité. Toutefois, nous n'avons pas pu identifier si ces personnes étaient en mesure de nous donner une définition stable du droit à l'oubli numérique, ni ce à quoi cette définition renvoyait pour elles.

8. Le droit à l'oubli numérique est déjà suffisamment traité dans la loi « Informatique et liberté » de la CNIL. La loi « Informatique et libertés » est reprise très majoritairement dans les chartes informatiques des entreprises.

- *Privé_SSII_1 :* « Les éléments dans lequel on peut le (droit à l'oubli numérique) retrouver sont uniquement le respect des recommandations de la CNIL relatives à la conservation de données à caractère personnel après un certain délai ».
- *Public_Univ_6 :* « Juste pour poser quelque chose par rapport au droit à l'oubli et à la loi Informatique et Libertés, le droit à l'oubli, vu de notre côté – je dirais, mais peut-être que c'est discutable –, c'est complètement intégré dans la loi Informatique et Libertés ».

Plusieurs règles énoncées dans les chartes sont considérées comme relatives au droit à l'oubli numérique. Ces règles concernent le respect et la protection des données à caractère personnel.

Respecter les données à caractère personnel se traduit dans la réalité à deux niveaux :

- Une obligation des entreprises à informer l'ensemble des personnes (personnels de l'entreprise, clients, partenaires) des données qui sont collectées et de leur délai de conservation. Les entreprises s'engagent ainsi à supprimer les données collectées à l'expiration du délai de conservation.
- Un droit des personnes à faire valoir, sur leur demande explicite, des droits d'accès, de rectification et de suppression de leurs données à caractère personnel.

Si les entreprises étaient en mesure de respecter l'ensemble de ces règles, le droit à l'oubli numérique aurait de fait une existence. Toutefois, faire appliquer ces règles au quotidien apparaît comme difficile. Si l'obligation d'information et le respect du droit d'accès aux données personnelles ne semblent pas poser trop de difficultés, le respect du droit de suppression des données et de leur délai de conservation sont quant à eux beaucoup plus problématiques. Les entreprises ne s'assurent jamais que les données ont été réellement supprimées à leur date d'expiration.

- *Privé_SSII_2 :* « Pour tout ce qui est "sauvegardes", non. On travaille en interne sur des serveurs, des supports encore externes ou ces trucs-là. Donc les supports, il en reste qui ont un certain nombre d'années ».
- *Public_Autre_3 :* « C'est qu'aujourd'hui, je n'ai aucune certitude, donc le risque est… enfin, ce n'est pas sécurisé que chaque service qui effectuerait un traitement particulier aille bien détruire les données au bout de telle période ».

9. Le droit à l'oubli numérique n'est traité que partiellement. La loi Informatique et Libertés et les chartes qui s'y réfèrent ne traitent qu'une partie du droit à l'oubli numérique.

- *Privé_SSII_1 :* « Non, je pense qu'on pourrait l'inscrire de manière plus précise, parce qu'effectivement, aujourd'hui, la charte informatique n'a pas été pensée en intégrant complètement tous les aspects qu'on peut avoir du droit à l'oubli. Maintenant, elle est plus orientée déjà, effectivement, sur le respect des données personnelles et la protection des données personnelles. Et donc, je pense que c'est un bon démarrage ».
- *Public_Univ_6 : C'est un* « bel outil » */…/ et un* « bon début » */…/, une loi avec* « beaucoup de potentialités » *mais qu'il faudrait compléter.*

Plusieurs pistes, problèmes ou manques sont évoqués :

- La seule destruction des données n'est pas suffisante, il conviendrait également d'effacer les traces d'utilisation d'un ordinateur et de consultation d'Internet.
  - *Public_Univ_6 :* « Les traces des consultations de toute utilisation ».
- Le fait de faire valoir son droit de suppression d'une donnée à caractère personnel peut s'avérer problématique et contradictoire lorsque la donnée en question est également une donnée publique.
  - *Public_Univ_6 :* « Par exemple, pour vous donner encore un autre exemple dans un autre champ, l'année dernière ou il y a deux ans – je ne sais plus – une étudiante nous a dit : "en telle année, j'ai été élue au CA…" – au CA ou dans un des conseils de l'université – "… pour le compte de tel syndicat. Je voudrais que mes propos soient enlevés des enregistrements, des comptes rendus et des ceci et des cela". Pour moi, c'est du droit à l'oubli. Qu'est-ce que je fais avec ça, moi ? D'abord, je peux dire… On peut botter en touche et dire : "tu n'es pas la CNIL"… Peut-être… Et encore. Il n'y avait pas d'enregistrement à l'époque, donc je peux botter en touche. Mais elle n'avait plus envie de… Elle avait dû changer d'opinion politique et elle n'avait plus envie qu'on voie… C'est légitime, mais qu'est-ce que je fais ? Si on me dit que c'est devenu un document administratif, que je n'ai plus le droit de le toucher, qu'il a été validé par le conseil d'administration, qu'il a été voté, qu'il a été approuvé par les membres, comment je fais pour aller le retoucher ? Enfin, je veux dire, concrètement, je peux, mais ça me pose quand même un certain nombre de questions ».
- Le traitement des données sur les réseaux sociaux est toujours aussi opaque et semble échapper à toute législation.

- *Privé_SSII_1 :* « Mais effectivement, c'est vraiment un domaine sur lequel on n'a pas, aujourd'hui, véritablement de contrôle. Aujourd'hui, je ne sais pas vous dire, en ce moment, combien de personnes sont en train de parler de notre société ou de parler d'autres choses sur des réseaux sociaux ».

Entreprises privées et entreprises publiques : des finalités différentes du droit à l'oubli numérique.

– Pour l'ensemble des entreprises interrogées, le respect de la loi Informatique et Libertés n'a pas pour finalité première de respecter le droit à l'oubli numérique. Il répond à d'autres considérations notamment légales.

Pour les entreprises publiques, il s'agit avant tout de protéger les données à caractère personnel et ainsi protéger l'usager et plus largement le citoyen. Il s'agit ainsi de ne pas conserver des données obsolètes et qui, selon leur contenu, pourraient nuire à l'individu.

- *Public_Univ_6 :* « Pour moi, le droit à l'oubli serait vraiment le droit des personnes pour la protection des données à caractère personnel, et qu'on s'assure bien qu'elles soient détruites au bout d'un certain temps pour une part, mais qui englobe aussi leur droit d'opposition – il a été donné –, leur droit de rectification et leur droit d'accès ».
- *Public_Autre_3 :* « Alors, la motivation, c'est aussi de protéger les données ».

Les entreprises privées se tournent vers une finalité différente relative aux problématiques de la divulgation des données. Prendre en compte le droit à l'oubli numérique c'est éviter le risque de divulguer des informations qui n'auraient pas dû l'être parce qu'elles sont soit personnelles soit obsolètes. En maîtrisant « *la mémoire de l'entreprise* » par la divulgation des seules informations autorisées, les entreprises privées désirent éviter le risque d'une mauvaise image auprès de leurs personnels, clients et candidats à une embauche.

- *Privé_SSII_1 :* « Le risque, c'est effectivement une image pas professionnelle et pas sérieuse vis-à-vis de nos clients, et puis à la fois un manque de respect et donc, du coup, de confiance des candidats que l'on souhaite attirer ». « C'est plus que l'oubli, mais en tout cas, la non-utilisation des données en dehors des finalités pour lesquelles elles ont été collectées »

Plusieurs difficultés de mise en œuvre du droit à l'oubli numérique ont été soulevées. Elles sont de plusieurs ordres : légales, techniques, humaines et organisationnelles.

10. Comment respecter l'obligation de déclaration des fichiers ? Sur le plan légal, la mise en œuvre du droit à l'oubli numérique devrait passer par le strict respect de la loi Informatique et Libertés. La difficulté est de cibler les traitements qui doivent faire l'objet d'une déclaration et/ou d'une demande d'avis (traitements avec des données sensibles comme le numéro de sécurité sociale par exemple). Ainsi, si le fichier et les traitements associés sont déclarés, le droit à l'oubli numérique est possible par le droit de suppression et de rectification. Par contre, la situation est toute autre si le fichier n'a pas été préalablement déclaré. Comment retrouver ce qui n'a pas été identifié et tracé ? En d'autres termes, comment oublier ce qui officiellement n'existe pas ?

- *Public_Univ_6 :* « Toute personne qui serait ici concernée par un traitement qui n'est pas déclaré, qui vient nous poser des questions de quelque nature que ce soit, ou demander un droit à l'oubli, une demande de suppression, gagne. Il a

raison par rapport à vous, même si normalement, c'est idiot. Il a raison, parce qu'à partir du moment où vous êtes en défaut en tant que responsable de traitement ici, vous êtes… »

- *Public_Autre_3 :* « Alors, non. La difficulté aujourd'hui qu'on a, c'est de cibler vraiment tous les traitements dont on a l'obligation de déclarer ».

11. Comment respecter de multiples règles internationales très divergentes ? Si sur le territoire français, les entreprises peuvent s'appuyer sur la loi Informatique et libertés, il existe un flou très grand (et les difficultés afférentes) d'un droit à l'oubli numérique dans les pays étrangers où elles ont leurs activités. Aujourd'hui, elles ne semblent pas disposer de solutions et agissent au coup par coup au fur et à mesure des situations nouvelles et des problèmes émergents.

- *Privé_SSII_1 :* « La CNIL a eu beaucoup d'échanges avec ses homologues européens pour essayer d'établir un certain nombre de règles, donc ça simplifie les choses lorsque la CNIL dit que tel ou tel pays a des règles de protection à peu près équivalentes, mais il faut savoir que par exemple, ça n'a pas simplifié les choses en termes de textes, de déclarations et de règles. Les règles restent très divergentes d'un pays à l'autre ».

- *Privé_SSII_2 :* « Mais je pense qu'on est dans un système où le droit est très complexe, parce qu'en plus, je pense que d'après les choses que j'ai vues, suivant les pays, les droits ne sont pas les mêmes ».

12. Comment financer la faisabilité technique du droit à l'oubli numérique des données internes de l'entreprise ? La faisabilité technique du droit à l'oubli numérique des données internes de l'entreprise est possible. Elle l'est d'autant plus avec les nouveaux systèmes d'information (moins de 5 ans d'existence) qui désormais intègrent des fonctionnalités de paramétrage pour permettre une gestion optimisée des données. Toutefois, cette mise en œuvre technique a un coût (non négligeable) ce qui suppose une véritable volonté politique interne pour la réaliser. Ainsi, les difficultés du droit à l'oubli des données internes résultent moins d'obstacles techniques que de contraintes budgétaires.

- *Privé_SSII_1 :* « Maintenant, techniquement, on n'en est pas loin. C'est-à-dire qu'en fait, je pense que… Oui, l'outillage existe. Maintenant, c'est beaucoup plus une question de moyens et de volonté de l'entreprise de travailler sur le sujet et de le mettre en place de manière rigoureuse ».
- *Privé_SSII_2 :* « Ça veut dire que c'est un service qui va coûter des choses et qui va rapporter pas grand-chose. Le tout, après, c'est simplement… Justement, comme vous le disiez tout à l'heure, après, ça pourrait être un avantage concurrentiel de dire : "chez nous, si quelqu'un n'est pas d'accord, l'info est…" »

13. Comment organiser la faisabilité technique du droit à l'oubli numérique des données internes de l'entreprise ? La mise en œuvre organisationnelle du droit à l'oubli numérique pose question. C'est notamment les problématiques de contrôle et de respect des processus et des règles afférentes qui semblent difficiles à réaliser. Ici encore, les difficultés du droit à l'oubli des données internes ne résultent moins d'obstacles techniques que de contraintes organisationnelles.

- *Privé_SSII_1 :* « Donc ça supposerait la mise en place de règles, de processus et de contrôler que ces règles et ces processus soient bien respectés ».
- *Public_Autre_3 :* « Non, mais ça pourrait être des données concernant des ressources, ou quand on croise, en fait, nos informations avec les informations d'une autre branche... Alors, ça se fait, par exemple, par nos contrôleurs, mais c'est vraiment encadré. Ça se fait par messagerie, il y a un cryptage particulier ».

14. Comment mettre en œuvre un droit à l'oubli numérique des données externes de l'entreprise ? Concernant les données externes des entreprises, les difficultés sont nombreuses et la mise en œuvre d'un droit à l'oubli numérique pour l'instant impossible. Ce sont principalement les pratiques sur les réseaux sociaux qui retiennent l'attention. L'opacité du fonctionnement technique de ces réseaux ainsi que leurs usages insaisissables font que les entreprises n'arrivent pas à faire valoir un droit à l'oubli numérique des données qu'elles souhaiteraient voir disparaître. Au mieux, elles essaient de « les cacher », de les enfouir. La suppression semble aujourd'hui illusoire par manque de traçabilité.

- *Privé_SSII_2 :* « Non, justement. Après, c'est "où est-ce que ça a été mis et qu'est-ce qu'on a comme moyens ?" Si c'est chez nous, on devrait pouvoir y arriver, s'il y a une trace quelque part chez nous. Si c'est sur le Web quelque part, sur des réseaux sociaux ou des choses comme ça, ce n'est pas du tout facile. Il faut retrouver... On s'occupe un peu de ça et justement, d'avoir de la veille par rapport... de l'e-réputation sur ce qu'on dit de nous... ». « C'est un service qui devrait être fait par chaque plateforme qui va héberger. Donc il faut que le service existe »

15. Comment mobiliser face au droit à l'oubli numérique ? Le droit à l'oubli numérique se heurte à un problème de formation et de connaissances des individus. Nombreux sont les personnels qui ne déclarent pas leurs fichiers personnels par ignorance. Nombreux sont les personnels qui ne s'interrogent pas non plus sur leur pratique en termes de divulgation de données (type de données transférées, destinataires à qui sont envoyées les données). La mise en œuvre du droit à l'oubli numérique est confrontée à un problème de comportement inadapté. Les entreprises interrogées ont donc insisté sur la nécessité de sensibiliser, de former les personnels mais également les citoyens aux problématiques larges du traitement des données. Il conviendrait ainsi d'une part de sensibiliser plus largement encore les personnels des entreprises à la nécessité de déclarer leurs fichiers et traitements associés ainsi que de déclarer les destinataires de ces données. D'autre part, il devient également nécessaire de sensibiliser les citoyens sur leur comportement mais plus encore de les informer de leurs droits (droit d'accès aux informations à caractères personnel, droit de rectification et de suppression).

- *Public_Univ_6 :* « Aujourd'hui, ça concerne tout le monde, de mettre en garde les gamins sur ce qu'ils mettent, sur leurs informations, leurs données... Là, c'est le minimum ».
- *Public_Autre_3 :* « Sensibiliser l'ensemble du personnel, c'est ce que je disais tout à l'heure. Sensibiliser. Du coup, cette sensibilisation va pouvoir aussi les interpeler sur "moi, dans mon activité, quand je fais telle chose, je suis en train de collecter ou de mettre en avant un traitement qui concerne des données, soit de salariés, soit d'allocataires, et attention : là, j'ai des obligations, et j'ai aussi, par rapport aux

personnes concernées, des devoirs, pour qu'eux fassent valoir leurs droits en cas de manifestation" ».

16. Droit à l'oubli numérique : vers de possibles effets délétères. L'application et la mise en œuvre du droit d'accès, de rectification et de suppression des données à caractère personnel, en conformité avec la loi Informatique et Libertés, peut être très lourd à mettre en œuvre. Elles peuvent aussi s'avérer dangereuses pour les entreprises françaises. Répondre à de telles demandes est possible mais très long voire fastidieux car les données sont parfois dispersées dans de multiples fichiers qui ne sont pas toujours clairement identifiés et référencés. Ainsi, si 1.000 personnes venaient à faire, en même temps, une demande d'accès, de rectification et de suppression de leurs données personnelles, une entreprise pourrait se trouver paralysée dans son fonctionnement opérationnel. Un droit à l'oubli numérique français pourrait alors devenir un outil de déstabilisation économique à la faveur d'entreprises étrangères.

Section 3 - Un droit à l'oubli numérique encore embryonnaire

À ce jour, s'il n'existe pas de droit à l'oubli numérique généralement et explicitement reconnu dans les chartes, il est aussi bien peu présent dans la pratique. En réalité, il y a un problème d'appréhension doublé d'un défaut de volonté de mise en œuvre.

Lorsque le droit à l'oubli numérique est présent, bien que partiellement, au sein des différents types d'entreprises, il fait l'objet de priorités différentes : les entreprises privées, soucieuses de leur image et de leur fonctionnement, axent la préservation des données sur cet aspect ; les entreprises publiques tendent plutôt à mettre l'accent sur les données de l'utilisateur comme objet de protection prioritaire. Cependant, toutes optent pour une nécessaire prise de conscience par les utilisateurs de la question sensible du traitement des données en général, et pas seulement de leur oubli.

La loi Informatique et Libertés constitue aujourd'hui le seul fondement juridique français véritablement connu et associé à la question du traitement des données. Mais cette loi est incomplète au regard du droit à l'oubli numérique et il manque un socle juridique plus explicite. Ainsi, de ce défaut d'encadrement législatif dérive le problème de la confrontation aux différentes règles internationales en la matière, puisqu'aucune uniformisation n'a eu lieu ou ne semble voir le jour.

Pour que le droit à l'oubli numérique soit effectif, il doit par ailleurs être techniquement soutenu par des moyens de mise en œuvre réalisables. A cet égard, les différentes entreprises consultées relatent uniformément la présence d'outils propres à l'application d'un droit à l'oubli numérique. En effet, celui-ci peut être promu au préalable par le biais du contrôle de la divulgation des données protégées par différents procédés, et de ce fait, par la possibilité envisageable d'en assurer la maîtrise, par la modification et l'effacement notamment. Cependant, si ces moyens sont réels, ils rencontrent des obstacles financiers et organisationnels qui empêchent une mise en œuvre cohérente généralisée et suffisamment efficace pour garantir une protection effective. De plus, le contrôle des accès externes reste à ce jour une question sensible pour les entreprises qui rencontrent de véritables difficultés à cet égard, dans la mesure où ils constituent autant de possibilité de fuite des données, par les différents réseaux sociaux et le développement du *cloud*

computing[11]. Enfin, une fois les données publiées, leur maîtrise s'avère particulièrement délicate, c'est pourquoi il est essentiel de les préserver au sein d'une sphère identifiable.

Afin que le droit à l'oubli soit une priorité, les différentes entreprises mettent lourdement l'accent sur la prise de conscience des utilisateurs, les sensibilisant à être responsables de leurs comportements vis-à-vis de leurs données personnelles, et/ou concernant les données des collaborateurs internes et externes à l'entreprise.

Cela étant, les entreprises doivent se soumettre à un certain nombre d'obligations propres à garantir l'existence d'un droit à l'oubli numérique. En effet, ces dernières doivent informer les utilisateurs des traitements qui sont effectués sur les données, sachant cependant que celles-ci doivent à cet égard demeurer identifiables. Elles doivent répondre aux demandes de modification ou de suppression des données que les utilisateurs sont en droit d'effectuer. De ce point de vue, les différentes entreprises consultées soulignent ici les difficultés de mise en œuvre pratique en raison des ressources limitées dont elles disposent pour mettre en application les demandes qui leurs sont adressées. Elles soulignent par ailleurs une mesure qui pourrait avoir un effet pervers pour les entreprises privées. En effet, les demandes d'effacement pourraient entraîner des conséquences délétères si elles étaient utilisées à des fins de déstabilisation économique par des entreprises étrangères qui ne seraient pas soumises au même droit.

Enfin, conscients de leurs obligations, les entreprises ne s'assurent cependant pas en pratique que les données ont été supprimées au terme de la prescription de leur conservation autorisée.

En cela, si l'idée d'un droit à l'oubli numérique n'est pas étrangère aux entreprises, qu'elles soient publiques ou privées, il ne fait cependant pas l'objet d'une priorité, parce que mal appréhendé, ou encore difficilement garantissable. De plus, il tend à être délaissé au profit de la seule protection plus générale des données à caractère privé.

Les résultats obtenus à l'issu de ce travail de recherche montrent que les entreprises privées et publiques n'ont pas encore fait preuve d'initiatives innovantes dans la mise en place de pratiques susceptibles de respecter un droit à l'oubli numérique. Aucune *soft-law* susceptible d'alimenter une future loi ou plus simplement de futures réflexions sur le droit à l'oubli numérique n'a été identifiée. Les entreprises se contentent de suivre la loi Informatique et Libertés sans volonté d'aller plus avant. Une future législation relative au droit à l'oubli numérique ne pourra donc vraisemblablement pas s'inspirer des pratiques de ces acteurs économiques qu'ils soient privés ou publiques.

Ainsi, nous pouvons affirmer qu'il n'y a pas aujourd'hui de base dans les pratiques des entreprises qui puissent être reprise pour être généralisée par un texte normatif sur le droit à l'oubli numérique.

---

11 L'informatique en nuage correspond à un procédé d'externalisation des données qui sont gérées par des entreprises externes proposant des services par des serveurs destinés à stocker des données.

CHAPITRE 2

Droit à l'oubli : Quel rôle pour le Délégué à la protection des données personnelles ?[12]

Le droit à l'oubli n'existe pas, pourtant cette expression est fréquemment utilisée, avec plusieurs acceptions. Cela entretient une certaine confusion, notamment avec les droits d'opposition et de rectification alors que le projet de règlement européen appelé à remplacer la loi Informatique et Libertés comprend la création d'un « droit à l'oubli numérique ». Le présente texte se focalise sur le rôle que devrait jouer le facteur d'auto régulation qu'est le Correspondant Informatique et Libertés et le futur « Délégué à la protection des données personnelles » dans la bonne application de ce nouveau droit, s'il voit le jour.

Section 1 - Aspect psycho social

I - Il n'existe pas à proprement parler de « droit à l'oubli » dans la loi informatique et libertés[13].

Il s'agit en fait d'une expression mais aussi d'une attente sociale, voire psychologique.
Pour les personnes qui l'emploient, l'idée qu'elle recouvre est l'obligation de prévoir une durée de conservation des données personnelles proportionnelle à la finalité du traitement. La CNIL vulgarise cette obligation sur son site Web par la mention « Les données personnelles ont une date de péremption. Le responsable d'un fichier fixe une durée de conservation raisonnable en fonction de l'objectif du fichier ».
A titre d'exemple, les fournisseurs d'accès à Internet (FAI) ne doivent pas stocker plus d'un an les adresses IP de leurs clients.
Cette vulgarisation peut poser problème car elle peut être mal interprétée par des non spécialistes (par exemple les consommateurs). Il s'agit d'une demande psycho sociale et non de la réelle connaissance d'un droit.
Tout un chacun peut comprendre qu'il détient un droit qui lui permet d'exiger en toutes circonstances auprès de tout organisme d'effacer toute information le concernant (« Oubliez tout de moi ! »).
Utilisée sans précaution, cette expression peut donc être source de litiges et de frustrations, car ce droit (ou ce qui s'en approche) ne peut être absolu.

Section 2 - Les textes

---

12 Par Bruno Rasle, délégué général de l'Association française des correspondants à la protection des données à caractère personnel.

13 Aucune occurrence dans le texte de loi Informatique & Libertés. Il ne semble pas non plus que le terme d'oubli existe dans d'autres textes de loi français.

Les textes existants sont-ils suffisants ? Doit-on mieux informer le public ou doit-on définir un nouveau droit ?

I - La durée de conservation : l'un des points fréquent de non-conformité

Contrairement aux idées reçues, il n'est pas possible de conserver des données à caractère personnelle sans limitation de durée : la loi Informatique et Libertés oblige le responsable de traitement à fixer une durée de conservation raisonnable en fonction de l'objectif poursuivie (la finalité)[14]. Cette durée doit être mentionnée dans la déclaration ou portée sur le registre en cas de désignation d'un CIL[15].

La CNIL a publié en 2005 une recommandation sur ce sujet[16], en spécifiant trois « zones d'archives » et les caractéristiques qui les différencient.

A l'usage, cette recommandation est difficile d'application, principalement par défaut d'outils (progiciels) adaptés et par les coûts nécessaires à sa mise en œuvre. Historiquement, cette disposition de la loi est l'un des plus difficiles à faire appliquer, les directeurs des systèmes d'information les plus vertueux étant le plus souvent dans l'impossibilité de veiller à son respect.

Quand il est désigné le Correspondant Informatique et Libertés (CIL) incite les Directions métier à mener une réflexion afin de formaliser la durée de conservation en archives courantes (celle liée à la finalité du traitement de données à caractère personnel concerné). En cas de désaccord il conseille le responsable de traitement sur ce point.

On note que certains CIL porte à leur liste des traitements non pas une mais deux durées de conservation : celle en archives courantes et celles en archives intermédiaires (zone dans laquelle les informations sont conservées dans l'hypothèse d'un litige).

II - Pour éviter toute confusion, il convient de préciser le droit.

On note une confusion possible avec les droits dits « de rectification » et « d'opposition ». Le droit de rectification permet de modifier les données et peut aller jusqu'à la suppression des données inexactes, périmées ou dont la collecte est interdite[17].

---

14 Cette contrainte n'existe pas outre Atlantique. Il est intéressant de noter que, malgré cela, la majorité des entreprises américaines prennent un grand soin à purger les données qui ne leur sont d'aucune utilité, par crainte d'être exposées à une forte charge en cas d'incident de sécurité (gestion des Data Breach). L'auteur de ces lignes fait le pari que les responsables de traitement européens seront plus attentifs au respect des durées de conservation dans l'hypothèse où le règlement appelé à remplacer la directive 95/46CE intègre une disposition de type Data Breach Notification.

15 On notera que cette information est peu fréquemment communiquée par la CNIL lors des demandes d'informations suite à l'exercice du droit de l'article 31.

16 « Archivage électronique dans les entreprises : recommandations de la CNIL »

17Article 40 : « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».

De même qu'il n'existe pas réellement de « droit à l'oubli », il n'existe donc pas de « droit à la suppression », alors que ce terme est relevé sur de nombreuses mentions d'informations des sites Web. La CNIL propose ce type de formulation afin d'informer les personnes de leurs droits :

> « Conformément à la loi informatique et libertés du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à .../...Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant ».

Il vaudrait donc mieux utiliser la formulation complète « droit de suppression des données erronées ou périmées » pour être sûr d'être bien compris.

De son côté, le droit d'opposition permet à toute personne de s'opposer – pour des motifs légitimes[18] – à figurer dans un fichier[19]. Il n'existe pas pour les collectes obligatoires (fichiers du secteur public comme, par exemple, ceux des services fiscaux, des services de police, des services de la justice, de la sécurité sociale, etc.).

Ce droit n'existe pas non plus dans le cadre d'un contrat qui lie, par exemple, une banque à son client. Le guide « La pub si je veux ! » de la CNIL comporte en sa cinquième page l'avertissement suivant :

> « Attention. Si vous avez souscrit un contrat auprès d'une société pour une durée prévue dans ce contrat, vous ne pourrez pas le résilier quand vous le voulez ».

Le droit d'opposition peut s'exprimer par un refus de répondre lors d'une collecte non obligatoire de données[20], par la possibilité de s'opposer à la cession ou la commercialisation d'informations[21] ou par la faculté de demander la radiation des données contenues dans des fichiers commerciaux.

Dans son document la CNIL utilise également l'expression « le droit d'être radié d'un fichier » dans deux cas de figure : afin que ses coordonnées ne figurent plus dans les fichiers de prospection, afin qu'elles ne soient pas mises à disposition d'organismes extérieurs à des fins de prospection.

Ce même guide précise que s'il est possible de demander à une société dont on ne souhaite plus être le client dans le futur de lui demander de procéder à « la radiation des informations vous

---

18 Il s'agit là d'un point de débat en lui-même : qu'est-ce qu'un « motif légitime » ?

19 Article 38 : « 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. Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur ».

20 Certaines personnes utilisent une autre stratégie qui consiste à polluer les bases de données marketing en fournissant des réponses erronées.

21 Dans la réalité, il existe de nombreux exemples où cette faculté n'est pas réellement offerte aux personnes concernées, ou bien d'une façon qui de respecte pas l'esprit (exemple : Pour passer commande d'un bien ou d'un service, il faut obligatoirement donner son accord pour une transmission de ses données aux partenaires de l'offreur).

concernant figurant dans ses fichiers ». La CNIL précise que cet organisme devra toutefois conserver dans ses archives les informations comptables liées à l'exécution du contrat pendant dix ans, en application de l'article L.123-22 du code de commerce[22].

On note deux limites au droit d'opposition :
- Pour qu'il puisse être exercé au moment de la collecte d'informations, la personne concernée doit en être informée et consciente de ses droits ;
- Pour qu'il puisse être exercé plus tard[23], en s'adressant au responsable du fichier, la personne concernée doit pouvoir identifier facilement celui-ci et être en mesure d'exercer réellement son droit d'accès.

Enfin le décret n°2007-451 du 25 mars 2007[24], précise dans son article 96 que « l'intéressé est mis en mesure d'exprimer son choix avant la validation définitive de ses réponses ».

III - Le « droit à l'oubli » est un élément d'une chaine. Il ne s'agit pas d'un droit isolé mais d'un « droit de suite ».

Il constitue un complément du droit de suite, qui constitue lui-même un complément essentiel du droit d'accès, celui-ci ne pouvant être réellement opérationnel sans respect du devoir d'information des personnes.

Avec action de la personne concernée, la chaîne est ainsi constituée[25] : Information, Droit d'accès, Modification ou mise à jour, Suppression des données erronées ou périmées.

Pour être valide, l'étude du « droit à l'oubli » doit donc se faire en tenant compte des interactions avec les étapes précédentes, car son effectivité en dépend en grande partie.

IV- Pour les fichiers commerciaux, le droit d'opposition peut se traduire par des « désinscriptions »

Le droit d'opposition (article 38) peut s'exprimer par la faculté de demander la radiation des données contenues dans des fichiers commerciaux, à tout moment et sans justification (on note ici une grande différence avec le droit d'opposition de la Loi Informatique & Libertés qui peut se faire « pour des motifs légitimes »).
Il s'agit là de rendre du pouvoir à la personne (« Consumer Control »[26]) et d'instaurer la confiance : la collecte de données personnelles est plus aisée et de meilleure qualité si la personne concernée

---

22 On notera ici les distinctions entre les notions de « ne plus figurer dans les fichiers de prospection » et « ne plus figurer dans aucun fichier de l'entreprise ».

23 Ce que la CNIL vulgarise sur son site Web par « Sachez aussi que même si vous étiez d'accord au départ pour fournir des informations vous concernant, vous pouvez changer d'avis et demander à ne plus être fiché ».

24 modifiant le décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004

25 Hors action de la personne concernée, les données doivent être purgées « naturellement » à la fin de la durée de conservation déclarée ou inscrite au registre (en cas de désignation d'un CIL).

sait qu'elle peut, à tout moment et facilement, modifier ses données et même se désinscrire. On note ainsi que certains acteurs permettent à leurs prospects et clients de gérer eux-mêmes, en ligne, leurs propres données. En France, l'expérimentation MesInfos, menée par la Fing[27] et à laquelle participe l'AFCDP[28], en est une illustration.

Cette faculté se retrouve également, concernant la prospection directe par courrier électronique, dans l'article 22 de la Loi pour la Confiance dans l'Economie Numérique :

> « Toutefois, la prospection directe par courrier électronique est autorisée si les coordonnées du destinataire ont été recueillies directement auprès de lui, dans le respect des dispositions de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'occasion d'une vente ou d'une prestation de services, si la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale, et si le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé. Dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé. »

Le texte LCEN n'est pas précis en ce qui concerne la rapidité avec laquelle la désinscription doit être effective[29].

Le code de déontologie de la FEVAD comporte à ce sujet la mention suivante :

> « Le professionnel maître d'ouvrage responsable de la collecte des données prendra en compte, ou s'engage à faire prendre en compte par ses utilisateurs, dans un délai de deux mois… les demandes de radiation ou de non mise à disposition à des tiers qui lui auront été transmises».

Le code de déontologie du SNCD, bien que plus précis concernant le traitement des désinscriptions, ne fait pas mention d'un délai souhaitable de prise en compte. Le GESTE (Groupement des Editeurs en Ligne) indique que :

---

26 Sur ce même sujet, le plan numérique pour 2012, présenté le 20 octobre 2008 par Eric Besson, alors secrétaire d'Etat chargé de la Prospective et du Développement de l'économie numérique, insistait sur l'importance de ce droit dans la protection de la vie privée : « l'internaute doit garder le contrôle de l'information diffusée », indique le point 45.

27 Fondation Internet Nouvelle génération fing.org

28 Association Française des Correspondants à la protection des Données à caractère Personnel www.afcdp.net

29 La réglementation fédérale américaine CANSPAM Act donne dix jours au professionnel pour prendre en compte les désinscriptions. On ne connaît que trop le ressenti de l'internaute qui continue à recevoir des messages plus d'un mois après sa demande. Le texte américain fait également obligation aux professionnels de conserver opérationnel le moyen de désabonnement un mois après l'envoi des messages.

« La demande [de l'internaute] doit être prise en compte dans les meilleurs délais et sa désinscription doit lui être notifiée dès qu'elle est effective ».

Avec cette disposition, l'internaute reprend du pouvoir. Le meilleur instrument à sa disposition réside dans sa capacité à se désinscrire. Tout repose donc sur l'efficacité des mécanismes de désinscription et de la confiance accordée par les internautes.
Sur le terrain, les choses ne semblent pas idéales : D'après les derniers tests effectués quant à la conformité de Google Latitude, service basé sur la géolocalisation, la firme californienne continue à localiser l'utilisateur même après que ce dernier se soit « délogé »[30] et des sanctions prononcées par la CNIL montrent que ces désinscriptions ne sont pas toujours prises en compte de façon totalement opérationnelle[31].

Section 3 - L'exercice des droits existants

L'organisation de l'exercice des droits existants est manifestement perfectible. Pour l'AFCDP, la désignation d'un CIL (Correspondant Informatique et Libertés) doté de réels moyens[32], accompagné d'une traçabilité des transferts de données à caractère personnel, doit s'imposer.

I- Le droits à l'information et le droit à l'accès aux données ne sont pas pleinement opérationnels

Malgré les efforts de la CNIL (qui propose sur son site un large choix de formulations), le devoir d'information, de la part du responsable du traitement, reste perfectible, dans le fond et la forme (cas des mentions difficilement trouvables sur un site Web).
La CNIL attache à raison une grande importance à ce droit initial, car il rend possibles les suivants (droit d'accès, de rectification, d'opposition).
Ainsi la CNIL a prononcé, le 26 février 2009, une sanction pécuniaire d'un montant de 40.000 euros à l'égard de la société DirectAnnonces pour « pratiques déloyales vis-à-vis des particuliers annonceurs, puisqu'ils n'étaient pas informés de la collecte et de la vente de leur annonce et, par conséquent, ils ne pouvaient pas s'y opposer ».
Le droit d'accès[33] permet à toute personne d'interroger le responsable d'un fichier pour savoir s'il détient des informations sur elle et le cas échéant d'obtenir communication de l'intégralité des

---

30 Pourtant, d'après la CNIL, « L'utilisateur de Google Latitude peut désactiver ou suspendre le service à tout moment ». CNIL, Contrôler Latitude,
http://www.cnil.fr/la-cnil/actu-cnil/article/article/91/controler-latitude/.

31 Début 2008, la CNIL a été saisie d'une douzaine de plaintes de personnes ayant rencontré des difficultés pour exercer leur droit d'opposition auprès de CDiscount. Quel que soit le moyen utilisé, lien de désinscription figurant sur le courriel, courrier postal ou appel téléphonique, les désinscriptions n'étaient jamais réalisées. La CNIL a donc mis en demeure la société de prendre en compte, de manière efficace, systématique et immédiate, le droit d'opposition à recevoir de la prospection commerciale.

32 L'AFCDP a apporté son soutien à une thèse professionnelle réalisée dans le cadre du Mastère Spécialisé « Informatique & Libertés » de l'ISEP et qui portait sur les moyens nécessaires au Correspondant Informatique et Libertés pour accomplir ses missions.

33 Nous nous limitons au droit d'accès direct.

données la concernant. L'exercice du droit d'accès permet de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer les données erronées ou périmées.

Ce droit a également donné lieu à sanctions[34].
Les travaux des participants au Mastère Spécialisé « Management et Protection des données à caractère personnel » de l'ISEP[35] montrent que seul un tiers environ des organismes sollicités répond à une demande de droit d'accès. Le pourcentage de réponses pleinement satisfaisantes est également décevant.
Il convient de noter que ce droit est encore très rarement utilisé par les personnes, par méconnaissance de leurs droits : en conséquence peu d'entités ont mis en place d'une procédure pour les traiter.
Le guide « La publicité si je veux ! » de la CNIL indique aussi que la personne peut demander « toute information quant à l'origine de leur collecte ». Il précise également qu'il est possible de demander à un organisme qui a réalisé l'action de prospection d'indiquer le nom de la société qui lui a fourni les coordonnées du prospect. Ceci sur le fondement de l'article 39.I.4 de la Loi Informatique et Libertés :

> « Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir.../... La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ».

On trouve de même dans le « Guide pratique du droit d'accès », publié par la Cnil en octobre 2006 le passage suivant :

> « Vous avez aussi le droit de connaître l'origine des informations vous concernant, c'est-à-dire d'où proviennent les données que l'organisme détient sur vous (par exemple, les a-t-il obtenues auprès d'une autre société, d'une autre administration ?) ».

II- L'exercice du « droit à l'oubli » se heurte également au phénomène de la « dissémination »

Lorsque l'internaute parvient à faire effacer ses données, rien ne garantit qu'avant cette démarche, le fichier contesté n'a pas déjà commencé à essaimer sur Internet. Identifier l'ensemble des traitements ayant relayé les données personnelles relève souvent de la mission impossible.

Concernant le droit de rectification, la CNIL précise que « le responsable du traitement doit prouver qu'il a procédé aux rectifications demandées et les notifier aux tiers à qui auraient été transmises les données erronées ». Cette obligation vaut également pour le droit de rectification.

Le décret n°2007-451 du 25 mars 2007[36] précise ce point en son article 99 :

---

34 La CNIL a, par exemple, prononcé une sanction pécuniaire à l'encontre de la société Neuf Cegetel sur ce fondement le 12 juin 2008.

35 Il est demandé aux étudiants d'exercer leur droit d'accès. Une promotion sollicite ainsi plus de 150 organismes.

36 Modifiant lui-même le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiées par la loi n° 2004-801 du 6 août 2004.

> « Lorsque des données à caractère personnel ont été transmises à un tiers, le responsable du traitement qui a procédé à leur rectification en informe sans délai ce tiers. Celui-ci procède également sans délai à la rectification », une logique qui se retrouve concernant le droit d'opposition, dans l'article 97 : « Le responsable du traitement auprès duquel le droit d'opposition a été exercé informe sans délai de cette opposition tout autre responsable de traitement qu'il a rendu destinataire des données à caractère personnel qui font l'objet de l'opposition ».

Encore faut-il voir connaissance des « tiers » auxquels les données auraient été transmises.

Lors de la transposition de la directive qui a donné naissance à la Loi pour la Confiance dans l'Economie Numérique, l'auteur de ces lignes avait regretté que l'indication de l'origine de la source ne soit pas obligatoire lors de prospection directe par courrier électronique[37].

Dans une lettre signée de M. Alex Türk et publiée sur la Toile[38] on peut lire la précision suivante :

> « A toutes fins utiles, je vous informe que l'internaute, dont les données sont transmises par la société A à la société B, doit être en mesure d'identifier l'ensemble des destinataires de ses données, pour que son consentement soit qualifiés d'éclairé. Ainsi, l'internaute doit se voir communiquer la liste nominative des partenaires et tiers de la société A à qui seront transmises ses données. Cette liste devra être mise à jour au moment du recueil du consentement de l'internaute et l'internaute devra, le cas échéant, être informé du caractère évolutif de cette liste sur le formulaire de collecte (ou sur la liste desdits partenaires en cas de renvoi via un lien hypertexte)».

Il semble que cette pratique n'ait jamais été observée dans les faits[39].

Certains acteurs du secteur de la communication directe vont au-delà du texte actuel et ont pris l'initiative d'indiquer la source de collecte quand ils réalisent un emailing pour le compte d'un tiers. Cette mesure participe également de la transparence et est facteur de confiance.
Il convient de noter que la loi Allemande entrée en vigueur le 1er septembre 2009 autorise exceptionnellement l'utilisation des données personnelles à des fins publicitaires sans accord préalable du consommateur si l'entreprise l'informe de l'origine des données utilisées. Le consommateur peut plus aisément exercer ses droits (d'accès, de rectification, d'opposition) auprès de la source, c'est-à-dire l'entreprise détentrice du fichier.

III - Il peut être intéressant de dissocier les différents cas de figure, selon que les données sont accessibles librement en ligne ou pas

Pour étudier le « droit à l'oubli » il nous parait utile de distinguer :

---

37 « Mais où ont-ils obtenu mon adresse ? » C'est, en toute logique, la première question que se pose un internaute à la réception d'un message publicitaire électronique.

38 http://www.pcinpact.com/actu/news/53221-cnil-base-mutualisee-accord-collecte.htm

39 Par ailleurs nous n'en avons pas trouvé le fondement juridique. Cette recommandation fait elle officiellement partie de la doctrine de la CNIL ?

- les données personnelles traitées en interne par des entités soumises à la Loi Informatique & Libertés (par exemples des entreprises à des fins de prospection) ;
- les données communiquées par l'intéressé et publiées sur des réseaux sociaux, des blogs, des newsgroups, des sites de partage de vidéo, etc.

Sans être nouveau, le débat sur les possibles effets négatifs pour l'individu des informations qu'il a lui-même diffusé en ligne est un sujet d'actualité avec l'essor phénoménal des services de réseaux sociaux[40]. Dans ce deuxième cas, l'expression « droit au regret » illustre parfaitement les attentes des personnes qui ont eu la légèreté de communiquer leurs données personnelles, qui s'en repentent et cherchent une issue.

Ce débat fait apparaître plusieurs problèmes :
- Les personnes ne sont pas forcément conscientes du périmètre d'applicabilité de la Loi Informatique & Libertés[41].
- Dans le domaine des réseaux sociaux et des moteurs de recherche, les grands opérateurs sont américains[42] : comment les contraindre à respecter la législation européenne ? Et quelle serait l'attitude du moteur de recherche chinois, Baidu ?

Outre ses actions au sein du Groupe Article 29, la CNIL cherche à faire passer auprès des populations concernées l'idée d'un « capital vie privée » qui se dégrade d'une manière irréversible, à mesure que nous en disposons sans modération (analogies avec le capital santé ou avec une aquarelle tenue à l'écart du soleil).

Les efforts de sensibilisation menée en ce domaine par la Commission sont à saluer, notamment pour éviter que des personnes révèlent des informations personnelles de tiers (photo d'une soirée trop arrosée mise en ligne sans l'accord des personnes y figurant).

Parmi les pistes de réflexion, on peut citer les démarches suivantes :
- Informer le public pour qu'il fasse de préférence usage de pseudonymes où qu'il utilise des services qui restreignent l'accès aux destinataires qu'il a autorisé ;
- Faire en sorte que les services tels que les réseaux sociaux, les sites de partage de vidéo proposent par défaut à l'utilisateur de fixer, au moment du dépôt, une durée de conservation au terme de laquelle le contenu sera détruit.

IV - la conformité à la loi sur tous les points précédemment évoqués est complexe, difficile et coûteuse

---

40 Le débat est apparu dès le début des années 2000 avec l'indexation des newsgroup et l'accès à ces newsgroup via les moteurs de recherche (Jeffrey Rosen « Unwanted Gaze – The Destruction of Privacy in America » 2000 – Arnaud Belleil « e-Privacy » 2001).

41 Il faut reconnaître que ce point est complexe, même pour les spécialistes.

42 L'approche américaine ne connaît pas le droit à l'oubli : aucune obligation de purger les données à l'issue d'une période de conservation légitime. Seule exception, très récente : en septembre 2013 lLe gouverneur du Sunshine State a signé une loi qui contraint les acteurs de l'Internet à retirer des contenus en ligne à la demande de mineurs (ils peuvent conserver les informations en base). L'obligation rentrera en vigueur en 2015.

Les avancées technologiques (courriers électroniques adressés à des destinataires multiples, sauvegardes et réplications, architectures techniques virtualisées, Cloud Computing, etc.) rendent difficiles et coûteuses la « purge » des données à caractère personnel au terme de la durée de conservation.

De même, très peu d'outils permettent de garder en mémoire ou de gérer facilement :
- l'origine et le contexte de la collecte (lors d'un salon, d'un rendez-vous, d'un échange d'email, à la suite d'une campagne marketing, etc.) ;
- les cessions ou mises à disposition des données à des tiers (par exemple à l'occasion d'opération d'emailing) ;
- les exercices de droits des personnes (accès, rectification, etc.).

Quand bien même ses outils existeraient, les informations ne sont pas disponibles pour les données actuellement en bases.

Il convient donc de prêter attention à l'équation économique et à ne pas créer une distorsion de marché en infligeant aux acteurs français des contraintes que leurs concurrents n'ont pas.

De plus, qui va supporter le coût des outils et des procédures ? La question porte ici sur la proportion entre les moyens à mettre en œuvre et l'utilisation par les personnes de leurs droits.

On notera également les différences qui existent avec des pays comme les USA, qui disposent de « Record Manager » et d'outils de « Content Management » conçus pour gérer des informations/données considérées comme un patrimoine et qui permettent une gestion temporelle (durée de vie pour chaque donnée, alerte sur atteinte d'une durée de référence, etc.). Il parait donc pertinent de recueillir la position des documentalistes et des archivistes sur ces questions.

Section 4 - Réflexion sur l'existence d'un droit au déréférencement

I- La projet de règlement européen introduit un « droit à l'oubli numérique »

Le projet de règlement européen du 25 janvier 2012 -ainsi que le rapport de M. Albrecht du 8 janvier 2013 mentionne clairement cette expression en son article 17 « Droit à l'oubli numérique et à l'effacement».

Cet article vient en effet préciser le droit d'effacement prévu à l'article 12, point b) de la directive 95/46/CE et fixer les obligations liées au droit à l'oubli numérique[43]. Entre autres obligations, est à noter celle incombant au responsable du traitement ayant rendu les données à caractère personnel publiques d'informer les tiers qui les traitent que la personne concernée a demandé l'effacement de tout lien vers ces données, ou de toute copie ou reproduction[44].

L'article 17 prévoit enfin le droit de limiter le traitement dans certains cas.

Voici les dispositions de l'article 17 de la proposition de règlement :

---

43 Cf. Explication détaillée de la Proposition de Règlement du Parlement européen du 25/01/2012 – page 10 de la Proposition

44 Considérant n° 54 de la proposition de règlement du Parlement européen du 25/01/2012 – page 29 de la Proposition

« I. La personne concernée a le droit d'obtenir du responsable de traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne les données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était enfant, ou pour l'un des motifs suivants :

a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe1, point a, ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement de données ;
c) la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19 ;
d) le traitement des données n'est pas conforme au projet de règlement pour d'autres motifs. »

Les débats autour de ce concept sont animés, car l'équilibre est délicat à trouver avec le devoir de mémoire, la liberté de la presse ou la liberté d'expression. Pour certains, ce droit serait « irréaliste et passéiste », tandis que pour des représentants des groupes de pression américains, ce projet représente « une grande menace pour la liberté de parole sur Internet ».

II - Quelle est la position de la CNIL ?

Si la Commission Nationale Informatique et Libertés ne s'est pas encore positionnée officiellement sur le sujet, plusieurs Membres de la CNIL se sont exprimés à l'occasion d'interviews. On y décèle le souhait que soit institué, dans ce cadre du règlement européen, un droit au déréférencement qui ne serait pas absolu, c'est-à-dire que la demande de déréférencement formulée par le citoyen concernant (certaines de) ses données à caractère personnel serait soumise à conditions de recevabilité. Madame Isabelle Falque Pierrotin s'est exprimée sur le sujet[45] en indiquant son souhait d'un droit au déréférencement qui permettrait au citoyen que ses données personnelles n'apparaissent plus dans les résultats des moteurs de recherche lorsque le droit à l'effacement a été reconnu pour le citoyen.

Edouard Geffray, secrétaire général de la CNIL, défend également cette position[46] : « Aujourd'hui, il y a un droit à l'effacement pour motif légitime. Le terme de droit à l'oubli n'existe pas dans la loi. En revanche, l'expression apparaît dans le projet de règlement européen en négociation à Bruxelles.

Pour la CNIL, il apparaît souhaitable que dans ce cadre soit prévu un volet déréférencement. Après il ne s'agit pas d'ouvrir un droit au déréférencement absolu. Est-ce que ce sera à l'autorité de contrôle d'apprécier le motif qui aboutit ou non à l'effacement ou au refus d'effacement ? Honnêtement, les débats ne sont pas encore consolidés pour avoir une mise au clair. »

---

45 France Info, Droit d'oubli sur Internet, Le droit d'Info, 12 avril 2012
46 Edouard Geffray, Secrétaire Général de la CNIL, PC Impact

Le site internet de la CNIL indique : « Le droit au déréférencement n'est, pour la personne qui remplit les conditions pour demander l'effacement de ses données personnelles, que le corollaire du droit d'effacement : il s'agit de pouvoir demander au moteur de recherche d'effacer totalement de ses résultats la donnée dont l'effacement a été obtenu, ainsi que ses répliques ».

III - Avant d'aborder le déréférencement, il nous faut définir la notion de référencement

Une page web est l'un des composants d'un site web. Wikipedia définit un site web comme « un ensemble de pages web hyperliées entre elles et accessibles à une adresse web (une URL) ». Il s'agit donc d'un ensemble de pages de textes, d'images ou vidéos, liées entre elles grâce à des hyperliens (ou liens hypertexte[47]) permettant de passer d'une page du site à une autre page du même site par un simple clic.

Dès lors, le référencement (ou l'indexation) d'une page web est l'opération permettant à une page

Web d'apparaître dans les moteurs de recherche.

Le contenu est référencé dans les résultats d'un moteur de recherche suite aux passages réguliers et automatiques des robots (spiders, crawlers, agents) de ce moteur de recherche, qui identifient automatiquement chaque page atteinte et la répertorient dans une base de données afin de la rendre accessible aux internautes à partir de mots-clés.

Les robots d'indexation visitent les pages toutes les deux à trois semaines. Toutefois pour certains sites d'actualité, la mise à jour peut être quotidienne.

En janvier 2012, il aurait été recensé plus de 600 millions de sites web.

Attention : certaines notions ne doivent pas être confondues :

a) Le crawl est l'opération par laquelle le robot piloté par un moteur de recherche trouve une page web. Le référencement (ou indexation) est l'opération consistant à répertorier certains sites web présents sur la Toile et à les faire apparaître dans les moteurs de recherche. En toute hypothèse un moteur de recherche peut décider de ne pas référencer une page Web que l'un de ses robots a pourtant « crawlée ».

b) Le positionnement consiste à ce que pour une expression de recherche, une page d'un site internet soit placée en bonne position, voire en premier, par les différents moteurs de recherche par rapport à d'autres pages Web contenant des informations similaires.

c) La suppression/purge des caches consiste en la suppression de l'information, du document, de la photo, de la vidéo sur le site Web d'origine, les réplications – dont les copies temporaires dans les proxy caches.

IV - Que cherche-t-on à obtenir via un droit au déréférencement ?

Le déréférencement absolu permettrait que des informations n'apparaissent plus du tout dans les moteurs de recherche en cas de requête.

---

47 Cf. Infra l'explication des liens hypertexte html

Il existe également une notion de déréférencement relatif, dans laquelle l'information figure toujours dans les moteurs de recherche, mais est positionnée à un rang tellement lointain qu'elle n'est jamais (rarement ?) consultée. Nous n'avons malheureusement pas trouvé d'étude indiquant quel était le « rang » à partir duquel on peut estimer que l'information ne sera jamais consultée par un internaute.
Des débats autour du projet de création d'un droit à l'oubli (la version en langue anglaise du projet utilise les termes de « droit à être oublié et à l'effacement ») est apparue l'idée qui ferait du droit au déréférencement une sous partie du droit à l'oubli. En quelque sorte le Droit à l'oubli serait la somme de l'effacement pour motif légitime et du déréférencement.

Voici un cas où le déréférencement aurait été apprécié (Affaire Marie C. Swallow[48]) :
A l'âge de 18 ans, une jeune femme avait participé à une vidéo pornographique, mise en ligne à son insu. Or, depuis, elle est devenue enseignante : Par sa décision du 28 octobre 2008, le TGI Montpellier (ord. réf.) Google a été condamné à désindexer toutes les pages diffusant la vidéo pornographique de la jeune femme, en application de l'article 38.1 de la loi Informatique et Libertés. Le tribunal a rejeté l'argument de l'impossibilité matérielle de la désindexation que présentait la société américaine. Etaient visées les requêtes « M. C. swallows », « M. C. » et « école de laetitia »
L'on notera que dans cette affaire, c'est le moteur de recherche de Google qui était concerné. Mais qu'en est-il des autres moteurs de recherche ? C'est une question importante, car si le déréférencement peut se définir donc comme l'action permettant à une page web de ne plus apparaître dans les résultats des moteurs de recherche, encore faut-il déterminer quels moteurs de recherche sont concernés…
Si Google est le moteur de recherche utilisés par la quasi-totalité des internautes français, les parts de marché diffèrent fortement au niveau mondial : 65,2% pour Google, 8,2% pour Baidu, 4,9%, pour Yahoo!, 2,8% pour Yandex, 2,5% pour Bing et 16,3% pour les autres moteurs de recherche.

V- Cas de l'Espagne vs Google

Voici un litige très intéressant, car il porte spécifiquement sur le droit au déréférencement. L'affaire remonte à 1998 : Un journal espagnol avait publié sur Internet l'annonce de la mise en vente d'une propriété immobilière, mise aux enchères suite à saisie pour défaut de payement des contributions de Sécurité sociale. Le texte comportait un lien sur le nom du débiteur. Celui-ci a argué que le délai de prescription était atteint pour ces faits.

La page était référencée par Google et positionnée dans les premiers résultats sur le nom de la personne.
Pour Google, le cas montre bien la difficulté à trouver un équilibre entre la liberté de la presse/d'expression et le droit à l'oubli.

---

48 Marie C. / Google France et Inc
http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3121

Pour pouvoir se prononcer sur le cas Google Espagne v/ AEPD (la « CNIL » nationale), la Cour nationale d'Espagne a demandé des clarifications à la Cour de Justice de l'Union Européenne (CJUE).
L'Espagne a prié la CJUE de lui apporter des clarifications ;

- sur la question de la territorialité (Californie ou Espagne ?) ;
- sur la question de savoir si une indexation est un traitement de données à caractère personnel ;
- si les droits des personnes concernées s'étendent au refus de l'indexation d'informations qui leur paraissent « négatives » les concernant, et ceci même si ces informations étaient/sont légitimes et exactes.

L'avocat général de la CJUE, Niilo Jääskinen, a publié un avis sur la question le 25 juin 2013[49] : « Une demande tendant à faire supprimer des informations légales et légitimes qui sont entrées dans la sphère publique serait constitutive d'une ingérence dans la liberté d'expression de l'éditeur de la page web ». Il estime que, dans le cadre de la Directive 95/46/CE, une autorité nationale en matière de protection des données ne saurait exiger d'un moteur de recherche sur internet qu'il retire des informations de son index, sauf dans des cas précis où des « codes d'exclusion » ont été inclus par l'éditeur, ce qui n'est pas le cas dans l'affaire en question.

L'avocat général souligne aussi que la directive européenne sur la protection des données n'établit pas de « droit à l'oubli » de portée générale, et qu'un tel droit ne saurait donc être invoqué à l'encontre des moteurs de recherche sur internet.

A la surprise générale, la CJUE n'a pas suivi l'analyse de Niilo Jääskinen et a donné raison à l'AEPD dans son arrêt publié le 13 mai 2014 (disponible sur le site Web http://curia.europa.eu, sous le titre « Arrêt de la Cour (grande chambre) du 13 mai 2014 (demande de décision préjudicielle de l'Audiencia Nacional - Espagne) – Google Spain SL, Google Inc. / Agencia de Protección de Datos (AEPD) (Affaire C-131/12) »).

Pour la Cour, « l'opération consistant à faire figurer, sur une page Internet des données à caractère personnel » doit être qualifiée de traitement de données à caractère personnel au sens de la directive. Elle va également dans le sens de l'Audiencia Nacional concernant la question de la territorialité. En clair, les personnes citées dans les moteurs de recherche ont le droit de demander directement aux moteurs de recherche la suspension des liens qui pointent vers des pages Web qui leur semblent ne pas respecter leurs droits.

Cette décision a immédiatement été entendue. Dans une interview qu'elle a donné au Monde le 20 mai 2014, Madame Falque Pierrotin, Présidente de la CNIL, indiquait « Nous avons reçu hier une demande de retrait de contenu citant la décision de la Cour de justice. ».

Le Groupe Article 29 a publié très rapidement un communiqué de presse[50] pour exprimer sa réaction sur cette décision de justice (chose assez rare pour être soulignée), et, dès début juin

---

49 http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077fr.pdf
50http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140523_wp29_press_release_ecj_google.pdf

2014, en réunion plénière, les autorités de protection des données européennes ont échangé leurs points de vue sur cet arrêt afin d'en analyser les conséquences et d'avoir une approche commune sur la mise en œuvre des conséquences de celui-ci.

De son côté, la société américaine a mis sur pied un groupe de réflexion afin d'être conseillée sur la meilleure façon de se mettre en conformité avec l'arrêt. Ce groupe comportait dix personnalités dont Eric Schmidt et David Drummond (Google), Jimmy Wales (fondateur de Wikipedia), Frank La Rue (Nations Unies), Peggy Valcke (Université de Louvain), José Luis Piñar Mañas (Université San Pablo de Madrid et anciennement AEPD), Sylvie Kaufman (Directrice Editoriale au journal Le Monde) ou encore Luciano Floridi (Oxford). Ce groupe, au nom de Google, a proposé aux internautes de lui donner leur sentiment sur le jugement de la CJUE[51].

Google a pris acte de la décision de la Cour et a posté en ligne un formulaire[52] permettant aux personnes concernées de faire part de leur demande : « Demande de suppression de résultat de recherche au titre de la législation européenne en matière de protection des données ». Le premier jour de la mise en ligne de ce formulaire de dé-référencement, Google aurait reçu plus de 10.000 demandes de désindexation, car il n'est pas ici question de « droit à l'oubli » mais bien de droit à la désindexation. Le lien incriminé sera certes retiré du moteur de recherche, mais les données en question ne seront pas supprimées pour autant. De plus, les recherches faites en dehors du territoire européen ne sont pas concernées par la mesure. En effet, le géant du web a des extensions pour plus de cent trente pays d'où il est toujours possible de chercher les liens qui ont été désindexés sur google.fr, par exemple. Techniquement, il s'agit d'un affichage sélectif en fonction de la version locale du moteur de recherche utilisée pour effectuer la requête.

Très rapidement sont apparus des historiques des liens désindexés, comme « hiddenfromgoogle.com ». Il est intéressant de noter que ce site contient l'avertissement suivant : « L'objectif du site internet est de lister l'ensemble des liens censurés par les moteurs de recherche dû au récent jugement sur le « droit à l'oubli » au sein de l'Union Européenne. Cette liste est une façon d'archiver les actions de censure de l'Internet. C'est au lecteur de décider si nos libertés sont respectées ou violées par le récent jugement de l'Union Européenne. ». Un débat s'est en effet rapidement ouvert sur le bien-fondé de certaines demandes de désindexation. Ainsi, début juillet 2014, le journal britannique The Guardian se plaignait de voir certains de ses articles ne plus être référencés par Google[53]. L'un d'entre eux évoquait le mensonge d'un ancien arbitre écossais pour justifier un pénalty. Plus surprenant, un autre portait sur le concours éphémère qui avait diverti les salariés de la Défense à l'été 2011. Le principe ? Coller à même les vitres des petites feuilles adhésives en réalisant les dessins les plus fous. Aucune des entreprises concernées n'étaient à l'origine des demandes de suppression d'un épisode qui aurait pu nuire au sérieux de leur image. C'est l'un de leur salarié qui a rempli le formulaire Google. Dans une interview, celui-ci a avoué s'amuser que l'article soit à nouveau sous la lumière des projecteurs après sa désindexation. Voici une parfaite illustration du fameux effet Streisand, selon lequel on court le

---

51 www.google.com/advisorycouncil

52 https://support.google.com/legal/contact/lr_eudpa?product=websearch

53 www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google

risque d'attiser toujours plus de curiosité à force de vouloir cacher des informations. Quelques jours plus tard, Google ré-indexait certains des articles en question.

Fin juillet 2014, le G29 rencontrait les représentants des principaux moteurs de recherche pour analyser la mise en œuvre pratique des principes clefs du jugement de la CJUE. L'objectif était de finaliser les recommandations du G29, en préparation. Celles-ci auront pour objectif d'uniformiser l'application du jugement en Europe, d'expliciter précisément la façon d'exercer ce droit au dé-référencement, de même que les refus potentiels de la part des moteurs de recherche. Les discussions au sein du G29 ayant montré la nécessité de permettre aux particuliers de comprendre les raisons précises pour lesquelles un moteur de recherche peut légalement leur refuser le droit au déréférencement, et de tenir compte, dans certains cas, de l'intérêt du public à accéder à l'information en cause.

Courant août 2014, à l'occasion d'une conférence, la Commissaire Européenne à la Justice, Martine Reicherts, est intervenue sur ce sujet : « Nous devons dépasser un débat faussé et adopter rapidement de nouvelle règles solides ». Elle estime que les détracteurs du droit à l'oubli tentent d'utiliser la décision de la Cour de Justice Européenne pour saper la réforme en cours, mais qu'il n'est pas question d'en profiter pour empêcher l'Europe de mettre en place une meilleure protection de ses citoyens ou de bloquer l'ouverture du marché unique numérique aux entreprises Européennes.

Il convient enfin de signaler la très intéressante demande de Hong Kong, à bénéficier du même traitement. En juin 2014, Allan Chaing Yam-Wang, le « Privacy Chief » du territoire, a demandé à Google d'étendre le droit au déréférencement imposé en Europe par la CJUE à toute la planète, « Nous vivons dans un village global. De nombreux ressortissants britanniques vivent ici et peuvent revendiquer le droit européen et se faire dés-indexer » a-t-il déclaré.

VI - Comment éviter de se faire référencer ?

Nous avons identifié quatre approches pour éviter qu'un contenu publié sur Internet soit référencé :

a) Ne pas respecter le standard utilisé par les robots : Cette approche est citée pour mémoire, sa mise en oeuvre technique exigeant un degré élevé de maîtrise technique (par exemple par l'utilisation du standard Web 2). Rien ne dit non plus que les moteurs de recherche ne modifieront pas leurs robots pour s'adapter à ces situations.
b) Prendre l'exact contrepied des techniques pour être bien référencé : Sous forme de boutade, un expert du positionnement fait cette recommandation et incite à utiliser des mots-clés clonés de nombreuses fois en fin de page avec la même couleur que le fond, à ne pas remplir les balises titres ni les balises alt des images, à ajouter de nombreux liens réciproques avec des link farms, à ajouter des pages satellites en abusant de toutes les techniques de spam indexing, etc.
c) Bloquer le crawl en indiquant la ou les URL des pages pour lesquelles vous souhaitez interdire l'accès. Pour cela, il faut publier ces directives dans le fichier robots.txt à la racine du site.
d) Ne pas empêcher le crawl mais positionner dès la publication une commande spécifique demandant aux robots de crawl de ne pas tenir compte de la page.

VII - Comment se faire déréférencer ?

Comme indiqué précédemment, le déréférencement est l'action permettant à une page web de ne plus être présente dans les moteurs de recherche.

Dès lors, pour que la page web (ou le site web) n'apparaisse pas dans les résultats des moteurs de recherche, il faut permettre aux robots d'avoir accès à ces pages avec la consigne « ne pas indexer ».

Pour ce faire, plusieurs techniques peuvent être utilisées :

a) Installer sur le site Web une balise meta robots noindex : Sa syntaxe est <meta name= « robots » content « noindex, nofollow, noarchive »/>. Si l'on souhaite indiquer les consignes à un seul moteur de recherche plutôt qu'à tous les moteurs de recherche, il suffit de remplacer le mot-clé « robots » par le nom du robot d'indexation du moteur visé (ex googlebot noindex).

b) Pour un site hébergé sur serveur Apache, le webmaster peut insérer l'en-tête http-x-robots-tag : avec le mod_headers activé (il suffit de rajouter la ligne ci-dessous dans le fichier .htaccess : Header set XRobots-Tag « noindex, nofollow »).

Il ne faut pas oublier si besoin de « débloquer le crawl »... pour permettre aux robots de lire ces balises ! Paradoxalement, si l'on veut prévenir tout affichage d'une page web dans les résultats, il faut justement laisser les robots accéder à la page en question. C'est le seul moyen de pouvoir leur donner la consigne de ne pas l'indexer dans les serveurs du moteur de recherche.

Ces actions sont-elles efficaces et suivies à la lettre ? Selon certains, « Si les grands robots respectent à la lettre les directives, il faut savoir que d'autres ignorent les interdictions, ou pire encore utilisent ce fichier pour avoir connaissance des zones interdites qu'ils vont fouiller ». Donc comme on peut indiquer les pages à exclure, des robots (mal intentionnés) peuvent aussi les trouver et les fouiller avec quelques lignes de code.

Attention : Ces précautions ne valent que si action est prise rapidement, avant que des liens soient créés. En effet, il faut noter que même la présence d'un robots.txt empêchant l'indexation complète d'un site Web n'empêchera en rien l'apparition du site dans la page de résultat d'un moteur si un ou plusieurs liens pointent vers celui-ci. Pour être efficace, un éventuel texte d'application devrait donc aussi prévoir une obligation pour les responsables des sites Web ayant établi ces liens, de les retirer.

Les liens hypertexte en langage html permettent de faire la liaison entre des pages de sites différents ou du même site : en cliquant sur celui-ci, une nouvelle page du navigateur s'ouvre. Dès lors, si des liens sont créés d'un site vers un autre, ce dernier sera affiché dans les résultats d'un moteur de recherche malgré le travail d'un robot.txt, comme l'indique clairement ci-dessous le moteur de recherche Google :

On voit apparaître ici une notion très importante. Si les précautions n'ont pas été prises dès l'origine et que l'information a été repérée et que des liens pointent sur elles, ce sera beaucoup plus difficile...

Comment faire pour savoir si des liens html pointent sur la page qui doit être déréférencée ? Pour ce faire, il convient d'utiliser la syntaxe « link : url ».

Si l'on a réussi à faire déréférencer la page en question, mais que l'information apparaît toujours sur Internet car elle figure encore dans des caches, il faut alors faire une demande de suppression des pages auprès de l'équipe du moteur de recherche. Google met à la disposition des

webmestres de sites internet une procédure de désindexation volontaire pour demander la suppression du lien et du cache des pages supprimées[54]. Cette procédure nécessite toutefois de disposer d'un compte Gmail... et implique donc une collecte de données personnelles.
S'agissant des moteurs de recherche Bing et Yahoo! Search, les outils pour les webmestres sont disponibles à l'adresse http://www.bing.com/toolbox/webmaster/?cc=fr.

VIII -Quel lien avec l'effacement actuel ?

L'on peut concevoir aisément le droit au déréférencement comme la prolongation logique du droit à l'effacement pour motif légitime qui existe actuellement : une fois l'effacement accordé au citoyen, il semble en effet normal de modifier le contenu des moteurs de recherche et d'en supprimer la référence aux données effacées.
Notons que cette démarche d'effacement des données, si elle est plutôt simple lorsque la personne s'adresse au responsable du traitement desdites données, semble en revanche nettement plus complexe à mettre en œuvre en cas d'utilisation par un tiers de ces mêmes données...

En effet, la proposition de règlement prévoit en son article 17. 2 :

> « Lorsque le responsable du traitement visé au paragraphe 1 a rendu publiques les données à caractère personnel, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci. Lorsque le responsable du traitement a autorisé un tiers à publier des données à caractère personnel, il est réputé responsable de cette publication. »

L'on comprend aisément que l'obligation d'information des tiers pesant sur le responsable du traitement des données visées par la demande d'effacement n'est qu'une obligation de moyens, hors le cas où il a expressément autorisé les tiers. L'effacement des données, et par ricochet l'application du droit à l'oubli, seront donc techniquement difficiles à réaliser.

IX- Certains opérateurs interviennent déjà dans le domaine du droit à l'oubli

Ainsi Google a créé en avril 2013 un « gestionnaire de compte inactif » qui permet aux détenteurs de compte Google (Gmail, Drive, Google +, Google reader, YouTube, etc.) de décider de leur vie numérique post mortem. Ainsi, en cas d'inactivité du compte pendant une durée de 3, 6, 9 ou 12 mois et à défaut de réponse à un email d'alerte, les données de l'internaute seront, selon son choix exprimé préalablement, soit entièrement supprimées soit transmises à des proches.

X- Une jurisprudence encore hésitante

Une décision récente a posé que Google Suggest n'est pas un traitement de données à caractère personnel : En effet, ainsi en a décidé le TGI de Paris par une décision du 12 juin 2013,

---

54 http://support.google.com/webmasters/bin/answer.py?hl=fr&answer=164734

estimant que les suggestions formulées par Google ne constituent pas un traitement de données personnelles au sens de l'article 2 de la loi Informatique et Libertés[55]. En tapant son prénom et son nom, le plaignant se verra donc encore proposer les qualificatifs d'escroc, de « presse-citron » et de « mongolien ».

En juin 2013, la Cour de Cassation a jugé que Google n'est pas responsable des suggestions proposées par son moteur de recherche[56]. Lorsque des internautes saisissaient le nom d'une société de garantie, celui-ci était systématiquement associé à l'adjectif « escroc ». La 1ère chambre civile de la Cour de cassation a jugé que « la fonctionnalité aboutissant au rapprochement critiqué est le fruit d'un processus purement automatique dans son fonctionnement et aléatoire dans ses résultats, de sorte que l'affichage des « mots clés » qui en résulte est exclusif de toute volonté de l'exploitant du moteur de recherche d'émettre les propos en cause ou de leur conférer une signification autonome au-delà de leur simple juxtaposition et de leur seule fonction d'aide à la recherche » Google ne peut donc pas être tenu responsable de cette publication.

Cet arrêt semble opposé à ce qu'a jugé la Cour fédérale allemande. Par un arrêt en date du 14 mai 2013, la Bundesgerichtshof (BGH)[57] a statué en faveur du requérant et à l'encontre de Google : Le dirigeant d'une société reprochait à Google que la recherche de son nom soit associée aux termes « scientologie » et « fraude », et ce sans fondement. Considérant qu'il y avait là atteinte à ses droits de la personnalité, le demandeur a assigné le moteur de recherche aux fins de réparation à chaque association de ces termes à son nom. La BGH a estimé que si Google se retranchait jusqu'alors systématiquement derrière le rôle des utilisateurs de son moteur de recherche, il lui appartient dorénavant de faire preuve de vigilance en cas de signalement d'association erronée de la part d'un internaute.

Cette décision est à rapprocher d'un cas australien[58] : En novembre 2012, Google avait été condamné à verser 200.000 $ de dommage et intérêts à un particulier qui avait initié les poursuites en 2009 après que Google a refusé de supprimer des liens renvoyant vers des sites proclamant, à tort, qu'il avait des liens avec le crime organisé de Melbourne. Le jury de la Cour suprême de Victoria a établi que Google n'était effectivement pas responsable du contenu publié sur les sites résultant de recherches opérées via son moteur, mais ce, uniquement jusqu'au moment où le plaignant a émis une requête de filtrage.

A l'inverse, une habitante du Wisconsin a été déboutée par la cour fédérale d'appel de Chicago en mars 2013, après avoir attaqué Google pour des retours jugés obscènes et dégradant associés à son nom et prénom dans le moteur de recherche[59].

XI- Déjà une obligation d'éviter le référencement ?

---

55 http://juriscom.net/wp-content/uploads/2013/06/tgiparis20130612.pdf

56 Civ 1, 19/06/2013, pourvoi n°12-17.591

57 BGH, 14.05.2013 – VI ZR 269/12

58http://tempsreel.nouvelobs.com/medias/20121112.OBS8964/google-condamne-pour-ses-resultats-de-recherche-enaustralie.html

59http://www.generation-nt.com/google-juge-non-responsable-resultats-son-moteur-recherche-actualite-1704272.html

Sans attendre la promulgation du futur Règlement européen, certains responsables sont déjà contraints à prendre quelques précautions pour éviter le référencement d'informations spécifiques dans les moteurs de recherche.

Dans le cadre de la loi sur la sécurité du médicament et des produits de santé (loi Bertrand) du 29 décembre 2011, portant sur la transparence sur les liens entre professionnels de la santé et l'industrie pharmaceutique, le décret d'application (dit Sunshine) impose que :

> « L'autorité responsable du site internet public unique prend les mesures techniques nécessaires pour assurer l'intégrité du site sur lequel elle rend publiques les informations mentionnées à l'article R. 1453-3, leur sécurité et la protection des seules données directement identifiantes contre l'indexation par des moteurs de recherche ».

En clair, les cadeaux des laboratoires seront diffusés sur Internet, mais interdits de référencement.

Section 5- L'apport du CIL (et du futur dpo)

I- Quelques pistes à explorer

Plusieurs pistes méritent d'être étudiées afin de donner une chance à un futur droit à l'oubli numérique d'être effectif.

A- Inciter à la prise de conscience

Piste de réflexion : Faire en sorte que les services tels que les réseaux sociaux, les sites de partage de vidéo propose par défaut à l'utilisateur de fixer, au moment du dépôt, une durée de conservation au terme de laquelle le contenu sera détruit.
Avant de supprimer un document, le moindre PC nous demande « Vous êtes-sûr ? ». Ne peut-on inciter, de façon similaire, les Webmaster de sites sur lesquels il est possible de poster des images, des vidéos, des commentaires :

a) d'ajouter systématiquement une étape de type « Vous êtes-sûr ? Vous êtes prêt à assumer la responsabilité du texte ou du contenu que vous êtes sur le point de déposer ? Ayez-conscience également – et même si vous regrettez par la suite- qu'il sera quasiment impossible de supprimer ce contenu de la toile à cause du phénomène de dissémination propre à Internet ».
b) d'ajouter, pour le dépôt de photo et de vidéo, l'obligation de spécifier une durée de conservation (ou date de péremption), avec une valeur par défaut (dans certains cas, le webmaster peut imaginer un dispositif d'alerte de l'internaute à l'approche de cette échéance, la durée de conservation de l'adresse email vaudrait la durée de validité choisie par l'internaute).
c) d'inviter à une période de réflexion (pas de mise en ligne immédiate, mais différée) ;
d) de proposer de manière plus visible une fonction de type miroir (« Voici ce que le monde entier pourra savoir de toi ») ;
e) de proposer une confirmation avec invite de prise de connaissance des moyens pour maîtriser son exposition.

Cette approche ne demande pas de modification des standards et permettrait aux internautes de prendre conscience de leurs responsabilités et du caractère quasiment définitif de

leurs actions (même si cette initiative ne s'applique qu'à des sites soumis à la loi française, on peut espérer que la prise de conscience s'applique également quand l'internaute s'apprête à déposer un contenu sur un site étranger). Cette approche répondrait au concept de Privacy by Design.

B- Mieux maîtriser la mise en cache

Malgré la suppression de certaines données personnelles sur le site Web d'origine, les informations personnelles qui posent problème peuvent rester plusieurs semaines, voire plusieurs mois, accessibles sur la Toile car conservées par des caches intermédiaires[60].
Dans le protocole HTTP, les entêtes de type "Cache-Control" peuvent être utilisées pour spécifier des directives que tout système de cache doit appliquer. Parmi celle-ci figure le paramètre « Cache-Control: max-age=x » qui peut être utilisé pour spécifier le temps maximum pendant lequel un objet peut être conservé dans le cache[61].
Piste de réflexion : Cette approche est utilisée principalement par les webmasters pour les images (C'est même une recommandation, cf. « High Performance Web Sites: Rule 3 - Add an Expires Header »[62]). Pourrait-elle être renforcée et étendue à d'autres contenus postés sur les sites Web ? Pourrait-on inciter à la création d'une métadonnée (associée à la donnée à caractère personnel) qui spécifierait une durée de vie (forcément renseignée et d'une valeur maximal en relation avec la durée de conservation définie selon la finalité du traitement) ?
Cette approche répondrait au concept de Privacy by Design. Toutefois il faut se souvenir que l'actuelle loi Informatique et Libertés ne s'applique pas aux caches (cf. Article 4). Le texte qui sera issu du projet de règlement comportera-t-il une exclusion similaire ?

II - Le CIL, facteur de relations apaisées

Au sein des entreprises et des collectivités, nulle autre fonction que le CIL (ou le futur DP● prévu dans le projet de règlement européen) est à même d'appréhender toutes les facettes de la conformité Informatique & Libertés.
En amont, il peut orienter un projet concernant des données personnelles (Privacy by Design). En aval, il peut en assurer l'analyse et proposer des optimisations (Privacy by re-Design).
Concernant les droits des personnes (information, accès, rectification, opposition) au titre de la Loi Informatique & Libertés, le CIL peut :
- proposer des formulations compréhensibles par les personnes concernées, mais conformes au droit et susceptibles d'assurer la sécurité juridique du responsable de traitement ;
- concevoir ou aider à la conception des procédures adéquates ;
- en surveiller la bonne application ;
- agir en support des services opérationnels ;
- tenir des statistiques ;
- procéder aux analyses et en tirer conséquences et conseils au responsable du traitement.

---

60 Ces moyens techniques ne semblent pas tomber dans le périmètre de la Loi Informatique & Libertés (cf. son article 4).
61 Un paramètre similaire est utilisé pour définir la durée de vie des cookies.
62 http://developer.yahoo.net/blog/archives/2007/05/high_performanc_2.html

Il peut faire de même concernant les demandes de désinscription au titre de la LCEN. Lors d'opérations marketing mettant en œuvre des tiers (loueurs de fichiers, routeurs d'emails, etc.), il peut s'assurer du respect des contraintes et au respect de la prise en compte effective des droits des personnes[63].

Le CIL est indéniablement un facteur de « pacification » des relations entre une entité et ses clients/prospects/usages/patients.

Les organisations qui ont désigné un CIL et qui ont mis en place une procédure efficace de gestion des demandes de droits d'accès en témoignent.

Le CIL est donc l'acteur incontournable pour que les modalités concrètes de mise en œuvre d'un « droit à l'oubli » aient quelques chances d'être mises en place, notamment veiller à ce que les données personnelles soient purgées à l'issue de la durée de conservation et pour protéger les personnes contre le détournement de leurs données personnelles.

III - Droit à l'oubli numérique : quel rôle pour le futur DPO ?

Si un « droit à l'oubli numérique et au déréférencement » prenait corps, quel serait le rôle du CIL (ou du futur DPO – Data Protection Officer) ?

Suite aux réflexions menées par l'AFCDP, association qui représente les CIL et les professionnels de la conformité à la loi Informatique et Libertés, voici quelques pistes qui peuvent être imaginées concernant le rôle du CIL dans l'application d'un éventuel droit au déréférencement :

a) Formaliser une procédure avant toute publication comportant des données à caractère personnel sur un site Web, pour pouvoir décider de façon préalable de placer les robots de nonindexation ;
b) Réfléchir à la formalisation d'une durée de vie pour les éléments postés ;
c) Etudier la possibilité d'utiliser des métadonnées permettant la gestion des durées de vie et des purges ;
d) Se former sur les techniques de désindexation ;
e) Sensibiliser les Webmaitres/Webmaster ;
f) Créer une procédure de gestion des demandes de désindexation ;
g) Présenter le CIL comme point de contact pour les demandes de désindexation ou, *a minima*, le désigner comme garant de la bonne prise en compte des demandes et de leur gestion.

La désignation d'un CIL par tout organisme mettant en œuvre un ou des sites Internet/des réseaux sociaux devrait donc être fortement encouragée.

Conclusion

Si un droit à l'oubli numérique était créé à l'occasion de la promulgation du règlement européen appelé à remplacer la loi Informatique et Libertés, il conviendrait que celui-ci soit clairement formulé, afin de permettre aux délégués à la protection des données personnelles de veiller à son respect de façon opérationnelle afin de protéger la vie privé des personnes

63 Il peut arriver que des demandes de désinscriptions adressées au routeur d'email ne soient pas transmises au donneur d'ordre ou au maitre du fichier concerné, ou que celui-ci n'en tienne pas compte.

concernées mais aussi de maîtriser les risques juridiques qui pèsent sur les responsables de traitement.

Il conviendrait aussi que le rôle du Délégué à la protection des données soit explicité mentionné, afin de donner une chance à ce nouveau droit d'être effectif.

L'auteur : Bruno Rasle a participé à la création de la première entité française dédiée à l'optimisation des réseaux et à la gestion des performances en environnement IP et s'est consacré ensuite à la protection des données stratégiques. Auteur du livre « Halte au Spam » (éditions Eyrolles, 2003), il a été membre du groupe de contact anti-spam mis en place par la DDM (Direction du Développement des Médias, services du Premier ministre). Bruno Rasle est Délégué Général de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) et intervient dans le cadre du Mastère Spécialisé « Management et Protection des Données à caractère personnel » de l'ISEP (Institut Supérieur d'Electronique de Paris). A titre professionnel, il gère les sujets liés à la conformité Informatique et Libertés au sein de la DACSSI (Direction de l'Audit, de la Conformité Informatique et Libertés, de la Sécurité du Système d'Information) de la Cnaf (Caisse nationale des allocations familiales).

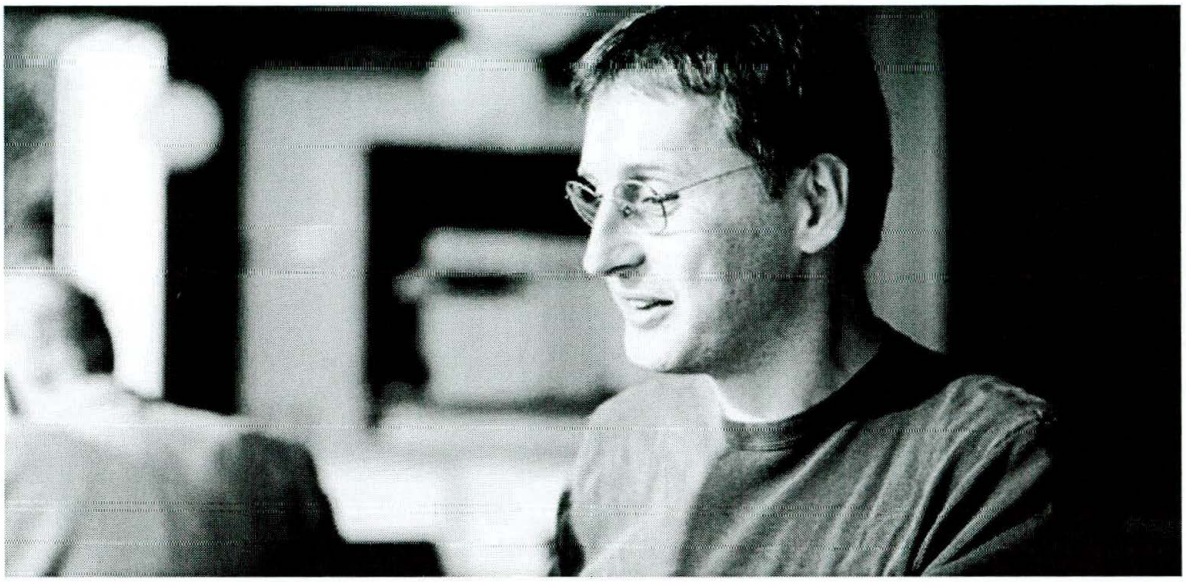
Cet article ne constitue cependant en rien une prise de position de l'AFCDP, mais présente uniquement une analyse personnelle de son auteur.

INDEX ALPHABETIQUE

(Le présent index renvoie à la contribution de chaque auteurs classés de A à L et par le numéro de paragraphe)

ANNEXES

Annexe 1: Interview with Viktor Mayer-Schoenberger



RESUME

Anciennement Professeur à l'Université d'Harvard, Viktor Mayer-Schoenberger est actuellement Professeur à l'Internet Institute de l'Université d'Oxford, où il enseigne le droit de l'internet. Fondateur de la société Ikarus, spécialisée dans la protection contre les virus, il est l'auteur de l'ouvrage de référence qui a initié le débat sur le droit à l'oubli : Delete, The Virtue of Forgetting in the Digital Age *(Princeton University Press, 2009). Dans cet opus, il explique pourquoi Internet va à l'encontre de la tendance des êtres humains à oublier ou, à défaut, à hiérarchiser les informations en fonction de leur contexte contemporain, tant et si bien que la persistance des informations sur la toile peut engendrer des dommages bénins, absurdes ou irréparables selon le cas pour l'image des personnes ou des entreprises. Sans plaider pour une faculté d'effacement* ad nutum, *il démontre de quelle façon un droit à l'oubli encadré pourrait pallier cet effet pervers de la technologie numérique sans remettre en cause ses immenses mérites et possibilités. Il propose à cette fin l'institution d'un système d'expiration des données par défaut, dont l'effet serait de prévoir d'une part l'effacement automatique de l'information mise en ligne par les internautes sur les réseaux sociaux, et, d'autre part, l'anonymisation sur demande dans les pages de résultats des moteurs de recherche après expiration d'un délai à déterminer en fonction des circonstances. Au cours de cet entretien, Viktor-Mayer Schoenberger reprend les termes essentiels de sa démonstration et explique l'intérêt, l'importance et le détail de ses propositions.*

Formerly a Professor at Harvard University (USA), Viktor Mayer-Schoenberger is currently Professor of Internet Governance and Regulation at Oxford University (UK), where he teaches Internet Law. The founder of *Ikarus Software*, a company focusing on data security which developed the software *Virus Utilities*, he is also a personal adviser to the Austrian Finance Minister on innovation policy. In his book *Delete, The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009), he explains how important forgetting is in life from psychological and social points of view, and why the 2.0 Web does not forget anything. He shows the long term negative consequences this lack of forgetting can have on democratic societies and Government, as well as on professional and private individual situations. At the end of his explanation, he suggests a couple of solutions to achieve real balance between the freedom of expression, access to free information and privacy. This could be developed through such mechanisms as the creation of an Expiry Date System which would have an expiry preset delay for any private information published on search engines and social networks. *Delete* has now become a reference book on the issue of the Right To Be Forgotten, and has developed into the starting point of any research in this field. Viktor Mayer-Schoenberger has also recently published in association with Kenneth Cukier *Big Data: A Revolution That Will Transform How We Live And Think* (Eamon Dolan Houghton Mifflin Harcourt, 2013) in which he explores the future consequences of the increasing capacity to combine vast and formerly separated collections of information.

How did you come to work on this topic?

Some years ago, I started wondering about what happens to the phenomenon of forgetting in the digital age of today. And I found that going into it was the very specific and important information privacy problem. I have studied privacy information problems for twenty years. I started in the late 80's, researching data protection issues, and became familiar with data protection legislation both in Europe as well as in the United States. I have written on it, and lectured on it. And I thought that with the end of forgetting in the digital age we might have a bigger information privacy problem... I wrote a short paper and published it. A lot of people became interested in the problem. Then a publisher called me and asked me to write a book and I said yes. As I carried out research for the book, I found that my privacy concerns were confirmed. But these concerns were not the only ones. There are other problems which arise when we give up forgetting, and they have little to do with privacy and they have much larger consequences to our society. That prompted me in my book to divide the concerns that I have with respect to privacy into two subsets. The first is to do with power, and the second is concerned with time. This idea of power deals with the connection between the individual and information, and whether the processor of information is the Government or whether it is a commercial entity. This imbalance in power has been the topic of data protection privacy for decades. Now the difference is that with comprehensive memory, I, as a data subject, may have already long forgotten that I provided personal information to companies, but they still have it, so that there is a real power imbalance between them and me. If I, as a person and data subject, realize that there is this imbalance, I might be prompted to say less than more. I might be prompted to self-censor myself in my communications and my exercise of free speech. This might have negative consequences on public discourse and democratic debate, because I might fear that in twenty years down the track what I say today might be held against me...

You might face one day the same kind of problem Dr Andrew Feldmar had to deal with[1]...

Exactly. Or for instance, I protested against certain things when I was a student. Of course, when you are young, you often protest against certain things... And fortunately, it is normally forgotten later on. It lets you evolve as a human being. Then there is the second subset: the dimension of time. And I am very concerned about it. The dimension of time focuses on how humans make decisions. Decision making is influenced by which facts we have in mind at a given point of time, and, by remembering these facts, or should I say forgetting them. Forgetting happens automatically when something turns out to be no longer relevant to our decision-making at that time. If something is no longer relevant, we forget it. But we are reminded about it, by for example an email that we read or an image that we look at. We begin the process of remembering something that we thought we had forgotten. We remember something previously irrelevant, because it is now relevant due to the photograph or the email we have in front of us. Our mind has now this formerly irrelevant but from that point on relevant piece of information, and it clouds our decision making. Most of the time, we forget past struggles or disagreements we have had, and that enables us to live and to deal with the present, and to look forward to the future. A problem occurs when we can no longer forget. Some people have been studied by cognitive psychologists, because of their difficulty to forget. It appears for them to be a curse, not a blessing, because all of their decisions of the past are continuously present. They are scared of making a decision, as they fear they will make the wrong one. Moreover, they do not have the ability to isolate or generalize about these past decisions, which is what we do in order to live. To live requires forgetting the details. Living with recall of all details entails no abstraction, and no generalization. That, of course, ascertains that we are unable to learn from our experiences. Jorge Luis Borges describes in a beautiful short story, *Funes the Memorious*, in his *Fictions*[2], the case of a man who cannot forget anymore and reads all the Latin and Greek classics, from A to Z, and remembers every word of them. As a result he cannot understand their meaning, because understanding necessitates forgetting the details. He can only see the tree, but never the forest. In that sense, non-forgetting is a real problem.

In one of his early works *On Aphasia* back in 1881, Sigmund Freud explained how aphasia was not due to a linguistic malfunction, but, on the contrary, by a weakness of the forgetting process, so that the person remains a prisoner of the last sentence they have said, just like a prisoner of past speech[3]. Do you think that in the light of this view we might have to face in the future, should we let this worldwide non-forgetting web continue its immense expansion, some kinds of behavioral or social troubles, as this 2.0 web will still drift in the opposite direction to our biological forgetting tendencies?

---

1 See above, F. Viangalli, p. & F. Girard, p.150 .

2 J. Borges, Fictions, Penguin ed, 2000, translated by H. Hurley, p. 91

3 See V.D. Greenberg, Freud and his Aphasia Book: Language and the Sources of Psychoanalysis, Cornell University Press, 1998; and Freud's original study: On Aphasia, A Critical Study, Literay Licensing 2011

That is the second big challenge. Remembering challenges our ability to decide and live in the present, as well as to project into the future. With too much remembering, we remain hooked to the past and we cannot cut that umbilical cord that we have with the past. That is one of the fates we might face. The other problem that I see is that if we, as human beings, begin to realize that our mental recollection of the past is not perfect, then we might begin to trust more the digital recollections of the past than our own recollection. We might trust this digital image more than our own mental images. This imbues a sense of originality and authenticity to the digital artefact that it may not have, as if we consider that "it is written on the web, so it is true". As we know everything that is digital can be easily manipulated, and there is no authenticity of the photograph on Flickr, for each photograph can be changed. Take a look at David King's book, *The Commissar Vanishes* (1997)[4], to see how an original photograph of Stalin with three of his comrades, was then modified each time one of these comrades fell from grace. The comrades were progressively erased, so that in the end only Stalin remained in the official photograph. This leads to changing the past by retouching a photograph. Of course, we might think that this is crazy, and that it is only communist madness from the past, and could definitely not exist in of our lifetime. But today, in the United States, there are companies to whom you can send your digital photos and ask to have your ex-partner erased. What does it have to do with memory? You take a look at a photograph of your holidays in Hawaii, but your ex-partner is not there anymore. Do people then create a new memory around this? Does that mean that you ex-partner was not present at that time? Herein lies the problem.

This brings to mind the famous experiment conducted by Drs Rade, Gary, Wade & Lindslay in 2002[5]. They demonstrated how easy it was to create false childhood memories. They showed people a single false photograph among real childhood pictures, and people started to believe that they remembered perfectly the situation in which the picture was taken, while, in reality, no picture was actually taken because it never happened...

Loftus and Pickrell made the same kind of study[6]. They asked people whether as a child they had ever been lost in a mall, and 22% of Americans said that they had been lost one day and remembered this today as a dramatic experience, while in reality only 1% of the respondents actually had become lost. This is indeed a curious phenomenon. If you ask about the past in a certain way, it makes the brain create something and reconstructs our memory. Such is our human mind. The problem for us is that digital memory is just as malleable and manipulable as the human brain. So if we begin to trust digital memory more than our human memory, we will trust what it is not more trustworthy.

Do you consider the cases of Dr Feldmar and Stacy Snyder as rare digital accidents, or do you think this kind of tragedy can potentially happen to anyone?

---

4 D. King : The Commissar vanishes, The Falsification of Photographs and Art, Metropolitan Books, 1997

5 Wade, K.A.; Garry, M., Read, J.D., & Lindsay, D.S. A picture is worth a thousand lies: Using false photographs to create false childhood memories.". Psychonomic Bulletin & Review, 2002, 9: 597–603.

6 E. Loftus F, J. Pickrell : The Formation of False Memories, Psychiatric Annals, 1995, 25 (12): 720.

It can happen and it does happen a lot. Wherever I go, and whenever I make a speech, everybody has a story to tell. Everybody comes up to me afterwards to tell me what has happened to them, for instance how they got fired from their job because of what they tweeted... I have heard so many stories like that, because as more and more people go online and behave in a particular way, these kinds of conflicts occur. I believe the reason for this is that many people misconceive of the available tools. They believe that posting on Facebook or Twitter, for instance, is similar to speaking in private. So they write as they talk in private, and think what they type is ephemeral. When a person says to a friend orally "I drank too much last night", it is private and ephemeral speech. But when the sentence is moved to the digital world, it is no longer ephemeral - it is recorded. That is what usually people do not understand. They behave on Facebook as they behave in the real world, and that is how they get into trouble.

But do you think digital abstinence can be a proper solution, or do you consider it as a mere impossibility?

I believe digital abstinence is a possible solution but one that would imply to forgo all of the benefits of the digital tools we have. If we want to go back in time, with a lot of resilience it is possible. But do we want to? No cell phones, no computers, etc. This would repeat in a certain manner the views of Pol Pot who deliberately said "I want to go back two thousand years in time", and ordered the execution of all those skeptical individuals who read books. In fact, going back in time usually leads to brutality and bloodshed. Honestly, let's forget that.

However, digital memory is quite potentially unlimited, and it remains something that we do not know how to deal with. Everything can be recorded for all time. Is that not a serious problem?

It is a very interesting question. The amount of information which is recorded every year is increasing significantly. A large majority of the information recorded every day in the world is digital, not analog. 99% is digital, while only 1% is analog. Ten years ago, 25% was digital, and 75% analog. The ability for humans to store information is also increasing, so that there is enough room to store all that we need to. In fact, as soon as we create enough room to store the information, we fill it up. Thus, more and more information will be recorded. However, I would be crazy to say everything will be recorded, for that would be technically impossible. Physics tells us that the act of recording requires energy, and energy creates entropy as a disorder somewhere else. Astrophysicists tell us that the Universe is increasing the amount of information, while on the other hand this information is information about disorder, not information about order. So if we ask whether our capacity will always be sufficient to record everything, the answer is negative. Of course we must be able to differentiate the use of the term "information" in physics, and to use it in the sense of the field of information technology, but the problem appears somehow to be the same from this particular point of view.

If we consider the case of the data an ordinary person sends digitally, can we say that every email they sent last year is still archived?

In fact, every single query has been archived. About 3 billion queries per day are archived, as well as each search result that is clicked on. Every mistake you have made writing your search query is also recorded. Google Translate has learnt a lot from that. Google has the world's best

spellchecker, an automatic spellchecking machine, because it learns from your mistakes. So when you type and make a mistake, it provides you with the search results it thinks are correct - it autocorrects your mistakes. When you click afterwards on these results, you confirm that you did in fact make a mistake because your show your interest for a result that the correct typing would have led to.

So should we perceive this as if search engines were some kind of spying technologies?

There's a difference between what we might call a private investigator or a detective, and a spy. Google is the perfect private investigator, because everything that you can find is combined with other relevant information. But they are not spying on people because there is no real intrusion into the life of web users. They certainly analyze your emails, but you are in principle told that they will do so.

Maybe one of the consequences of this worldwide Panopticon might lie in the need to have in the future a real strategy to build ourselves our own digital reputation. What do you think about this e-reputation concern?

For individuals as for companies, an e-reputation has become a real parameter of any professional success. In the US, this digital dimension of your reputation is terribly important. When you are applying for a certain job, you may have to give your username and password of your Facebook account to the human resource office.

That is terrible. What happens then if you refuse?

You don't get the job. In fact, you don't even get an interview for the job.

But if you do give this information, they will look at your profile and everything on it...

Exactly. They will look through your account and screen everything as far as they are worried about your digital reputation.

It clearly appears to be Orwell's 1984!

They require you to be intruded upon. Google and Facebook, themselves, are not intruding into your privacy. It is you who is required by companies to permit such intrusion. They just want to check whether you have any skeleton in the closet, whether you have done anything bad. This is the reason why my students have two Facebook accounts: a professional one, and a private one. This brings us back to Erving Goffman's work[7], back in the 50's. He explained how people have at least two stages to act on: a front stage and a backstage. He described it through the analogy of a waitperson in a restaurant who is very kind to you. She is very kind indeed to you as a customer, but if you discreetly go to the kitchen you will probably hear her speaking in a completely different way, using other expressions, and maybe swearing, shouting, etc. What Facebook does is to combine the front stage and the backstage into one single stage, and people feel very uncomfortable with that. That is why my students create two accounts, a front stage

7 See for instance E. Goffman : The Presentation of Self in Everyday Life, Penguin ed. 1990

account and a backstage account. Or three accounts or potentially more for all the multiple stages they want to play on. But what they do not do is to combine them into one dossier, in order not to be the private detective who puts everything together. We should be able to keep apart our private life, our professional life, our sport club life, etc.

That is what famous artists do. They have a professional profile on Facebook, which is not their private one. And it is often managed by their agent. For instance, if I take a look at, let's say, David Bowie's available profile on Facebook, it will be for sure the professional one.

But what is interesting is that it is prohibited to do this according to the Facebook terms of service. They do not allow you to have more than one profile. So if you want to do so, you have to choose two different names and two different emails. In other words, you have to use avatars. Why is Facebook not clamping down this? Because since Facebook went public and being sold on the stock exchange, they had to show an increase in activated accounts, so they no have little interest in stopping the double profile practice.

Do you think a proper education would be sufficient enough to prevent the problems arising out from a non-forgetting web?

No, I don't. Education can change people's values. For instance, the previous generations, those of our parents or our grandparents might have been homophobic and reactionary against homosexuals, and today we no longer perceive homosexuality as they did. But what we are required to do in order to act in a world of omnipresent memory is not to change our values but to change our decision making process, so that old things become less important or relevant. It is biologically impossible, or, to say the least, it requires evolution rather than education.

What about people's attitude towards the problem? Do they even know it exists?

More and more people have begun to understand and anticipate the problem. Two years ago, colleagues of the University of Berkeley in California did a survey among Americans. They asked various questions about privacy. One of the questions was "Do you want the Congress to implement a Right to Be Forgotten?" Expectedly, 90% of the 60 year old and more section said yes. But, surprisingly, 84% of the 18-25 year olds also said yes. Across the generations people now feel that there is too much memory.

Back in the 60's, Bruno Bettelheim wrote a famous article in which he prophesied the end of privacy in the future[8]. Do you think his prediction has finally turned out to be real?

Not at all. Our desire to remain partly private, our desire to have our own private realm, whether it is physical or virtual, still continues. People are worried about the information they have placed online. Every year, studies show that a significant portion of ecommerce does not take place because customers do not want to endanger their personal information. There are so many instances where people want to keep their private life private. The desire to privacy has not

---

8 Bruno Bettelheim : The Right to Privacy is a Myth, Saturday Evening Post, July 27th, 1968.

declined. It has remained constant, because, in fact, privacy is a human need. The problem is that we do not yet understand the long term consequences of the digital tools now available.

Let's talk about the remedies against these new forms of privacy violation. Do you look at avatars as a proper protection for people in this field? Does an avatar provide effective protection, without any new RTBF?

I think avatars are not the solution to this problem. It is just a hacking of the system. By using avatars, you cheat. So it cannot be the whole solution. It is only a quick-fix solution that does not last. Take a look at the Netflix case[9]. Netflix is a video rental company in the US. On the previous version of Netflix, if you signed up, you could select which DVD you wanted to watch. They sent you the first DVD of your personal list at home, and once you had sent it back to them, they shipped the next on the list and so on. The price was about 20 or 25 $ per month. Now Netflix has become an entire digital service, but previously the service was physical and they used to ship physical records. One feature of the service was to recommend which movies you should personally watch next. In order to improve their recommendation engine, they once added a public contest. The goal of the contest was to provide the best algorithm to predict customers' preferences. In order to have the test dataset available, they selected a couple of million transactions from five hundred thousand customers, made the data anonymous by deleting everything, except the identification numbers and information on the hours and the time of watching the movies, and made this available to researchers. Within two weeks, a researcher from a University in Texas had re-identified a woman in the Midwest in the United States and outed her as a lesbian. How did they arrive at this conclusion? In fact, the woman had made a mistake. She had used avatars. She had written rating reviews of the movies she had seen on Netflix, but she also had written the same reviews on IMDb, using exactly the same language, the same words. That's all... by analyzing the reviews, it was easy to identify the person. That is the problem with having multiple avatars. Using avatars does not prevent you from leaving clues of your identity.

So whatever you do behind your avatars, you leave some kind of a digital fingerprint...

Exactly. Having several avatars requires us to act in a very strict manner in order to separate our lives. But our lives are never that perfectly separated, so that we might betray some information here with an avatar that will make it possible to link it with another avatar. When it happens, this hacking of the digital memory does not work anymore.

Then avatars cannot protect you against linguistic recognition systems.

That's precisely the reason why they cannot be a proper solution to the problem. We must find something else.

What about the services provided by e-reputation agencies? They create some digital content such as articles, websites, posts, statutes, photographs or blogs, in order to scroll down the page rank of any information you don't want people to know about you.

---

9 See W. Aspray & P. Doty, Privacy in America, Interdisciplinary perspectives, Scarecrow Press, 2011, p.40

It works and it is for sure a useful tool. But the problem is that you have to pay for it. Companies and rich people can do that, but not everybody can do so due to financial constraints. So the question is: shall we give privacy to rich people only? Shall we give a good reputation only to the rich? I don't think so. Privacy is a human right.

The problem may also lie in the very relative effectiveness of the law, when it has to deal with the net, and especially with huge companies such as Google, Facebook, Twitter, etc. Do you believe in the effectiveness of the law in this matter? Are mandatory rules useful in this field?

I think this discussion about the ineffectiveness of the law is based on a misconception. A lot of engineers used to ask for 100% perfect law enforcement. I don't. We do not need 100% law enforcement. Law as a general matter of principal is never completely enforced up to a level of 100%. If you go on the highway, some people might keep the speed limit and go faster. But if 85 - 90% of people comply with the rule, it is already enough for society to function normally. So the real question is "Will we achieve 85 - 90% compliance"? Google and Facebook account for about 70% of the traffic on the internet. So if we get only Facebook and Google to comply with the law, we already have 75% compliance. One must also know that if we get Google to comply with the law in this matter, then technically Microsoft will certainly follow, for instance. If you do not appear in the first, the second and the third page of results on Google, as a big company, then practically you disappear. So long as Google is such a powerful gatekeeper to get information, having Google comply with the law is already a great victory.

But Google earns money recording everything. They analyze the data, and sell them to companies. If a regulation should prescribe to delete or slow down the page rank of information on a person's demand, that could also slow down their advertising revenues. Is that not a threat for search engines business?

Not significantly. First of all, Google is receiving a significant portion of its advertisement revenues from Europe. A lot of European companies pay to get ads on Google. So if Google had to close all its services and offices in Europe and just go back to California, they would lose much more money. That is not an acceptable proposition for them: they would lose about 30% of their revenues. That would be economic suicide. What is important for Google is to come up with the solution which takes care of the problem and at the same time does not expose them to additional risk. So if we say to Google "This is a mechanism we want you to implement. If you do it, you can continue to do what you did previously, and you will not be sued in Court", we will offer them a valuable advantage: legal certainty. The real question is to find the workable mechanism that will provide a significant or sufficient forgetting service. But such a mechanism will certainly not destroy search engines.

The EU directive on personal data was adopted in 1996. At this time, the problem you describe in your book had not yet occurred. Do you think time has come to rewrite the directive?

Time has come potentially. But when I look at the draft regulation, it is not about rewriting it. Of course, the draft regulation mentions in its Article 17 a RTBF, but as it is expounded, it appears to be a mere re-statement of the rights individuals already have had by virtue of the directive. It is

not something completely new. It is only a small expansion, or, if you prefer, an update. That is why I disagree with a lot of critics that have been made on the RTBF to indicate that it will undo the entire web and make it impossible for Google to provide its services.

In your book, you propose to create an Expiry Date System (EDS). Could you explain how this system would work?

Certainly. I suggest that the tools which are already available give us an opportunity to add an expiration date to all the personal information we store, so that once the expiration date is reached, the information is deleted from the system. You could change the expiry date at will to keep something longer or shorter if you wanted to. For instance, imagine you upload a photograph to Facebook. With EDS, you would have easy access to settings allowing you to add an expiration date to this picture particularly, if you want to modify the predefined expiration date already set. Later on, once the expiration date has come, the uploaded photograph is automatically deleted from Facebook.

Would such an expired photograph be really deleted, or would it rather be unavailable to web users?

To me, it doesn't matter much. What I am mainly worried about is mainly public exposure. I also fear, nonetheless to a very much smaller degree, that Google still retains the photograph on some of its services. Given the complexity of the structure of the internet, it is almost technically impossible for Google to totally destroy a photograph and ascertain whether it has vanished forever. What is important is that the photograph is clearly unavailable to any normal public access, and that it is absolutely unlawful to show it again for the person who still has it.

From a legal point of view, do you suggest to create a new action of Tort?

On the basis of law, we already have legal possibilities to sue any digital aggressor who might publish a picture or some private information without any consent of the person, in violation of data protection law. The mechanisms exist. The real problem is that people do not use them. I have personally looked at twenty years of case law in German data protection law. I have asked everybody if they knew of cases, and nobody has a single one. Nobody has sued on this basis for such facts.

What about the Max Mosley case[10]?

In fact, Max Mosley did not ask Google for money. He just wants information to be deleted.

Let's imagine a real RTBF is now implemented, so that any person could ask for an expiration of their personal data on Facebook and Google. Do you think that reconstruction websites such as Way Back Machine would threaten the efficiency of this new deleting function?

---

10 See above : F. Viangalli, p. 133 & F. Girard, p.150

They don't. Interestingly enough, when you go to Way Back Machine and ask them to delete an ancient version of your website, they do it. They act in a very pragmatic manner so that their service cannot be regarded as an obstacle to justified forgetting.

What about newspapers?

The problem lies in newspapers archives being available on line. Here we must differentiate between newspapers that act responsibly and those that do not. The *Guardian*, in the UK, for example, is a responsible newspaper. If somebody asks *The Guardian* to destroy some now old information published ten years ago, because it is today damageable for this person, they will consider it. Of course, the information is still written in the paper version. However, ten years after the fact, most of the people will take a look at the online version, and not go to the library and look for the original paper version. That is the way we should analyze this. They don't rewrite history, for they remove the name online, put an asterisk instead and specify it was done on the person's request. But they also pay tribute to privacy in this manner. That is a good balance.

However, e-reputation agencies face more problems with private bloggers. Some of them can be stiff and reject vigorously any demand of deleting personal information previously published on the web. What can be done?

Here lies one of the main differences between the analog world and the digital world. In the analog world, a person who has been attacked would try to refute an accusation. In the digital world, you try not to react to it, waiting for it to be buried by the next digital avalanche that occurs. This changes completely the way we look at information.

Some people say that the creation of a RTBF would be the first step towards state control of the web. Do you fear such an unwanted drift?

My answer to this statement is that the absence of a right to privacy is precisely the beginning of control by commercial or governmental entities on our privacy. Back in the 30's, there was a significant discussion among constitutional and civil rights lawyers. The dilemma was to know whether some rights are more important than others. This debate is turning up again now in its modern form when values such as freedom of expression on the net are looked upon as having superior value compared to privacy for instance. Or when certain people who published personal information are looked upon as having a more important position than the people the information was about. In Germany, after the Second World War, the *Grundgesetz*, the new Constitution, asserted that every single human right is equally important as each other. I really think it is a good way to think of human rights. There can be no ranking of rights. Thus, the freedom of speech is as important as privacy is on the ground of human rights: neither one is less valuable, nor more. They are equal. We need to find the right balance between them. If we don't do that, we open the door to fascist ideas and carry out a hara-kiri of human rights.

In 1968, Andy Warhol said in the catalogue of an exhibition at the Moderna Museet of Stockholm: "I believe that in the future everyone will be world-famous for 15 minutes". Don't you think a RTBF would go against the natural human inclination to parade and publish statutes, images and so on?

That is true, but only in a certain way. People want to be looked at. However, when later on it has become too much for them, they actually want to be forgotten. They want to take themselves away from the situation. The RTBF will help them when they are exhausted from being seen, because of serious inconveniences.

Do you think in the future we shall have a new web, based on contextualizing search results? Is such a contextualized web a real possibility or do you perceive it as a utopia?

I hope we will have a more contextualizing web. I am encouraged in this matter by what internet engineers and researchers tell me each time I discuss this problem with them. Some of them have told me for example how they plan to color in information on search results pages, so that an old result will appear in grey, with a short note to explain the temporal context of this result. It can be seen as an interesting idea to change the user's experience of digital tools. However, if full contextualization helps, it does not solve the entire problem of the non-forgetting web. The Andrew Feldmar case is a good example to show why. In the US, the official questionnaire any immigrant must fill in when he arrives in the United States asks: "Have you ever trafficked in any controlled substance?" As you can see, it does not specify whether the substance has to be looked upon as a controlled one only if it was illegal at the time the person used it, or if it has to be regarded as illegal even if it was legal at this time since it is now forbidden by the law today. This question remains an interpretation problem for lawyers, which contextualized search engines will not solve on their own. The case of Dr Feldmar would not have been solved by a simple contextualization. The real problem will only be solved by a RTBF. That is why we definitely need to create it.

Interview conducted by François Viangalli (University of Grenoble, CESICE)

at the Oxford Internet Institute (Oxford University) on Dec 4th 2012

Annexe 2 : Traduction

Le droit à l´oubli numérique sur internet: l´expérience espagnole[1]

Introduction

Effacer des données personnelles sur Internet n´est pas impossible: au contraire, c´est une pratique viable et habituelle. L'activité de supervision de l'Agence espagnole de protection des données (AEPD) le montre, prouvant de manière incontestable cette pratique par ses nombreuses résolutions qui sanctionnent et obligent des responsables de sites Internet à supprimer des données qui étaient logées sans l'autorisation de leurs titulaires.

Mais la difficulté majeure est d'empêcher les moteurs de recherche de référencer les informations personnelles logées sur des sites web quand l'AEPD[2] en dispose ainsi.

Google [3] a refusé à plusieurs reprises d'exécuter les résolutions de l´AEPD, et par là-même de garantir le droit à l'oubli en invoquant les fondements juridiques qui sont brièvement résumés

---

[1] Traduction du texte du Professeur Artemi Rallo Lombarte par Mr Jacobo Rios, Maître de Conférences HDR en droit public Université de Perpignan Faculté de droit et sciences économiques

[2] En France, plusieurs arrêts ont imposé cette obligation aux moteurs de recherche. En mars 2011, un Tribunal de Montpellier a reconnu le droit à l'oubli contre Google d'une enseignante qui, en 2008, a découvert que les termes « Laetitia école », lorsqu'ils sont recherchés sur Internet, renvoient vers des vidéos amateurs pornographiques qu´elle avait fait quand elle avait 18 ans, où elle a été désignée comme une « porno star », La Cour a considéré que l'association de son nom constituait une atteinte à sa vie privée et a ordonné la suppression par Google (« Google, condenada en Francia a retirar enlaces a un vídeo pornográfico de una profesora », *El País*, 16 mars 2011). Encore plus important, le Tribunal de Grande Instance de Paris a ordonné à Google le 15 février la suppression de certains liens après avoir constaté l'existence de liens pornographiques liés au prénom et nom. Il a déclaré que cette indexation constituerait un acte illégal portant atteinte à la vie privée, provoquant des dommages dans la vie professionnelle des personnes impliquées et une violation du droit d'opposition. La Cour, en plus de l'amende pour les dommages et le préjudice causé au demandeur, a ordonné le déréférencement du nom et prénom de tous les liens pornographiques sur le moteur de recherche (http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3362). Plus récemment, le 6 novembre 2013, le Tribunal de Grande Instance de Paris a ordonné à Google de supprimer les images de neuf photographies dans lesquelles Max Mosley, ancien président de la Fédération Internationale de l'Automobile, est apparu en 2008 vêtu d´un uniforme nazi en participant à des jeux sadomasochistes avec cinq prostituées - CHÉRON, A.: « Affaire *Mosley/Google* : liberté d'expression, atteinte à la vie privée et droit à l'oubli numérique », 12 février 2014 (*http://www.dalloz-actualite.fr/chronique/affaire-mosleygoogle-liberte-d-expression-atteinte-vie-privee-et-droit-l-oubli-numerique#.UvnYB_GY6g*)-.

[3] Le succès planétaire des services offerts par Google (en particulier, son moteur de recherche) et ses conflits récurrents avec la protection de la vie privée ont provoqué un traitement doctrinal abondant comme le montrent, à titre d'exemple, les ouvrages suivants: goldberg m.a.: "The googling of online privacy: gmail, search-engine histories and the new frontier of protecting private information on the web", *Lewis and Clark Law Review*, vol. 9-1, 2005, pp. 249-272; church, p. and Kon, G.: "Google at the heart of a data protection storm", *Computer Law & Security Report*, nº. 23, 2007, pp. 461-465; TENE, O.: "What Google knows: privacy and Internet search engines", *Utah Law Review*,

dans ce qui suit: 1) le traitement automatique du moteur de recherche se base en premier sur les mots-clés et en deuxième lieu sur la comparaison entre les mots inclus comme critère de recherche dans la consultation de l'utilisateur avec ceux de la liste; 2) le moteur de recherche est neutre par comparaison avec le webmaster qui est le seul capable de supprimer les informations ; 3) la loi espagnole ne s'applique pas parce que Google Espagne représente Google Inc. seulement dans la vente de publicité comme agent ou représentant commercial exclusif de Google Inc., mais sans responsabilité sur le moteur de recherche ; 4) Google Inc. fournit des services de moteur de recherche des États-Unis, de sorte que la Directive européenne de protection des données ne s'applique pas.

Cependant, l'AEPD a construit une base juridique permettant de développer un *modèle « espagnol »* de droit à l'oubli : 1) le droit d'opposition interdit le traitement des données personnelles s´il y a une raison légitime et fondée en référence à une situation personnelle particulière qui le justifie conformément à l'article 18 de la Loi Organique sur la Protection des Données (LOPD); 2) la loi espagnole s'applique lorsque le responsable du traitement des données n'est pas établi sur le territoire de l'Union européenne, mais utilise des moyens situés sur le territoire espagnol; 3) la loi espagnole s'applique lorsque le traitement est fait « dans le cadre des activités d'un établissement » du responsable qui implique l'exercice effectif et réel de l'activité, quelle que soit la forme juridique de l'établissement (un bureau local, une filiale avec personnalité juridique ou un tiers), comme lorsqu'un bureau est établi dans un État membre pour la vente de publicité visant les habitants de cet État; 4) les moteurs de recherche s'appuient sur des « moyens » dans le territoire de l'État membre quand, par exemple, les centres de collection de données sont situées sur le territoire de l'État, avec l'utilisation d'ordinateurs personnels, de terminaux, et de serveurs ou l'utilisation de cookies et de logiciels similaires.

Nous allons voir plus en détail les arguments avancés par Google et comment ils ont été contestés par l'AEPD.

Section I- La prétention à l´impunité [4] de google

I-L'application de la législation des États-Unis. Google Inc., contrôleur exclusif du moteur de recherche: ni « établissement » ni utilisation des « moyens » en Espagne

Les services de moteur de recherche de Google relèvent de la responsabilité unique de Google Inc, une société américaine constituée selon les lois de l'Etat du Delaware et dont le siège est en

---

nº. 4, 2008, pp. 1433-1492; MUTH, K.T.: "Googlestroika: Privatizing Privacy", *Duquesne Law Review*, vol. 47, 2009, pp. 337-353; DWYER, C.: "Privacy in the Age of Google and Facebook", *IEEE Technology and Society Magazine*, Fall, 2011, pp. 58-63; O'REILLY C.: "Finding jurisdiction to regulate Google and the Internet", *European Journal of Law and Technology*, vol. 2, nº. 1, 2011, pp. 1-13; RAKOWER, L.H.: "Blurred line: zooming in on google street view and the global right to priva<cy", *Brooklyn Journal of International Law*, nº. 37-1, 2011, pp. 317-347 ROSEN, J.: "'The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google'", *Fordham Law Review*, vol. 80-4, 2012.pp. 1525-1538.

[4] Comme l'indique J. R. REIDEMBERG: « the initial wave of cases seeking to deny jurisdiction, choice of law, and enforcement to states where users and victims are located constitutes a type of "denial-of-service" attack against the legal system. Internet separatists use technology-based arguments to deny the existence of sufficient contacts for jurisdiction and the applicability of rules of law interdicting certain behavior. From this perspective, the attackers seek to disable states from protecting their citizens online » (« Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, vol. 153, 2005, p. 1953).

Californie - et, en conséquence, tout litige sur les résultats de recherche (suivi, stockage ou indexation des données) sera soumis exclusivement à la loi américaine et la juridiction de Californie[5].

Google Espagne est une simple filiale de Google Inc., dont l'activité est limitée au marketing et à la vente de publicité en Espagne et, par conséquent, elle ne fournit aucun service relatif au moteur de recherche. Sur les deux prémisses précédentes et en évoquant des résolutions contraires[6] et favorables[7] à l'applicabilité du droit européen au moteur de recherche, Google Inc. a nié que Google Espagne puisse être considéré comme un établissement de la compagnie situé en Espagne et, selon les règles d'applicabilité territoriale établies aux articles. 4. 1 a) Directive 95/46 et 2.1 a) LOPD, elle renvoie toute la responsabilité de l'activité du moteur de recherche à Google Inc. dans le cadre exclusif de la loi américaine.

Google Inc. n´accepte pas plus « l´existence de moyens situés en Espagne » pour la fourniture de son service de moteur de recherche. Google Inc. Fournit ce service global au moyen de centres de données, qui ne sont pas localisés en Espagne et auxquels les utilisateurs espagnols transfèrent leurs données. Les « robots» ou « spiders » se trouveraient dans ces centres pour obtenir les informations des sites Web - si le webmaster responsable de l'information autorise l'envoi - et les indexent de manière automatisée. De telle sorte que toutes les procédures relatives à l'activité des moteurs de recherche se feront sur les équipements informatiques de Google Inc. mais sans recourir à des moyens techniques où l'information se trouve hébergée à l'origine.

Par conséquence, la loi européenne ou espagnole ne serait pas territorialement applicable du fait de ne pas avoir à « recourir à des moyens situés » en Espagne selon les termes prévus par l'art. 4. 1 a) de la Directive 95/46 et 2. 1 a) LOPD.

---

[5] Voir les Conditions du Service du moteur de recherche Google dans sa version du 1er mars 2012 (*https://www.google.es/intl/es/policies/terms/regional.html*).

[6] Dans la plupart des procédures résolues par l'AEPD, Google a fait valoir la position contraire d'autres autorités administratives et judiciaires nationales: 1´) une résolution du Garante italien pour la protection des données, du 11 décembre 2008, rejetant une demande d'annulation des données et reconnaissant que Google Inc ne se trouvait pas dans un État membre de l'Union européenne. 2´) Un arrêt du Tribunal de Grande Instance de Paris, 14 avril 2008, qui a rejeté les revendications d'un particulier contre Google Inc et Google France en se fondant sur le fait que le service de moteur de recherche est fourni exclusivement par Google Inc sans établissement ni usage de moyens en France puisque Google France agit uniquement sur le plan commercial. 3´) Un arrêt d'une Cour de première instance de Bruxelles, le 2 juin 2009, a rejeté la plainte contre Google Belgique qui lui attribuait la faculté d'annuler des résultats de recherche.

[7] Mais les résolutions antérieures, qui nient l'existence de la législation européenne, sont effacées par de multiples autres dans lesquelles les autorités administratives et judiciaire nationales estiment applicables la législation européenne au moteur de recherche Google dans des litiges relatifs à la fonction « auto-compléter »: 1) l'AEPD dans sa résolution 2647/2012 (TD/1105/2012) demande à Google Espagne de prendre des mesures pour prévenir l'association incorrecte des données d'un citoyen avec le terme «gay» dans son référencement de suggestion généré semi-automatiquement ; 2) un arrêt de la Cour de d´Appel de Paris, 18 décembre 2011, dans un litige entre Google et la compagnie d'assurance Lyonnaise de Garantie, a ordonné à Google de supprimer des suggestions - en particulier, le nom de la compagnie d'assurance a été associé avec le terme « escroc »; 3) un tribunal ordinaire à Milan a ordonné à Google de supprimer la suggestion qu' associe avec le prestataire les termes italiens « truffatore » (fraudeur) et «truffa» (escroquerie) ;4) plus récemment, en avril 2013, un tribunal japonais a condamné Google à retirer dans leurs suggestions le nom d'un citoyen associé à celui d'un groupe criminel; 5) et, en mai 2013, la Cour suprême d'Allemagne a contraint Google à supprimer le nom de famille d'un entrepreneur avec les termes « Scientologie » et « escroquerie » (El País, 15 mai 2013, p. 52).

II-La neutralité de l'automatisme des moteurs de recherche comme argument de l'irresponsabilité. Le webmaster comme responsable direct exclusif

La neutralité du service de recherche est, sans aucun doute, l'un des principes sur lesquels Google Inc. fait valoir son absence de responsabilité dans le traitement des données. À l'inverse, la capacité du webmaster de prendre une décision relative à l'indexation, le rend directement responsable et l´oblige à assurer la conformité de la publication avec les lois de protection des données.

En définitive, Google Inc. se dégagerait de toute responsabilité en considérant que les décisions concernant l'usage et la destination des données personnelles relèvent exclusivement de la responsabilité du webmaster qui rend possible l'accès à l'information. Autrement dit, seulement eux décident sur « les finalités et les moyens » de traitement de données [arts. [2 d) la directive 95/46 et 3 d) LOPD].

En sa faveur, Google Inc. affirme que l'Avis 1/2008 sur les moteurs de recherche en ligne, du 4 avril 2008, du Groupe de travail de l'Article 29, dans lequel le degré de responsabilité du webmaster est différencié de celui du moteur de recherche: « Le principe de proportionnalité exige que, dans la mesure où un moteur de recherche agit uniquement en tant qu'intermédiaire, il n'est pas responsable principal du traitement des données à caractère personnel. Dans ce cas, le principal responsable du traitement des données à caractère personnel sont les fournisseurs d'information »[8]. Toutefois, Google Inc. n'évoque pas le fait que ce même avis s'accompagne d'une responsabilité directe des moteurs de recherche relatif à la suppression des données personnelles référencées: « La responsabilité formelle, juridique et pratique qui incombe au moteur de recherche est généralement limitée à la possibilité de supprimer les données de ses serveurs. Pour ce qui se réfère à la suppression des données personnelles du référencement et des résultats de recherche, les moteurs de recherche ont une responsabilité suffisante pour être tenus responsable du traitement (seul ou conjointement avec d'autres.) ». Lorsqu'il y a une obligation de supprimer ou bloquer les données à caractère personnel, elle découle de la législation des États membres[9].

III-L'inefficacité du droit à l'oubli exercée uniquement par les moteurs de recherche Internet et le principe de proportionnalité

Google Inc. argumente que la demande d'une autorité administrative ordonnant exclusivement au moteur de recherche la suppression dans son référencement de renseignements personnels sera inopérante si, auparavant, le webmaster qui a publié l'information ne les supprime pas et/ou utilise des outils techniques qui empêche le référencement. De plus, si ces informations restent sur le web, elle pourra être accessible pour n'importe quel autre moteur de recherche ou plateforme Internet et restera par conséquent accessible au public.

---

[8]http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

[9] En particulier, l'Avis 148 cite dans la page n° 18 le cas de l'Espagne: "dans certains États membres de l'UE les autorités de protection des données ont réglementé spécifiquement l'obligation des fournisseurs de supprimer le contenu du référencement de la recherche, sur la base du droit d'opposition consacré par l'article 14 de la Directive sur la protection des données (95/46/CE) et la Directive sur le commerce électronique (2000/31/CE). En vertu de ces lois, les moteurs de recherche sont obligés de suivre une politique de notification et d'annulation semblable à celle suivie par les fournisseurs de services d'hébergement, afin d'éviter la responsabilité".

Google Inc. appelle donc à la nécessité de respecter le principe de proportionnalité, comme un principe fondamental du droit communautaire : « en vertu du principe de proportionnalité, le contenu et la forme d'action de l´Union ne peut pas dépasser ce qui est nécessaire pour atteindre les objectifs des traités » (art. 5.4 Traité sur l'Union Européenne), pour vérifier la conformité des résolutions de l'AEPD vis-à-vis de la législation et la jurisprudence européenne sur la liberté d'expression, d´information et d´entreprise (art. 11 et 16 Charte des Droits Fondamentaux de l'Union Européenne).

Google Inc. nie la capacité de l´AEPD en droit espagnol à résoudre le droit d'opposition qui force Google à supprimer les informations de son moteur de recherche au moyen d'une pondération de divers droits fondamentaux en lice: vie privée et dignité du demandeur, liberté d'expression et d'information de celui qui publie l'information et des tiers qui pourraient avoir accès, liberté d'entreprise du moteur de recherche.

Toutefois, comme Google Inc. le rappelle, la récente jurisprudence européenne - relative à la protection du droit d'auteur contre le téléchargement illégal sur Internet - oblige les autorités nationales à procéder à une pondération entre tous ces droits en conflit: « le droit communautaire exige aux États membres, lorsqu'ils adaptent ses directives à leur droit interne, de tenter de se baser sur une interprétation de ces dernières qui garantit un juste équilibre entre les différentes d'adaptation des droits fondamentaux protégés par l'ordre juridique communautaire. Ensuite, au moment d'appliquer les mesures d'adaptation de l'ordre juridique interne aux directives mentionnées, il appartient aux autorités et aux organes juridictionnels des Etats membres non seulement d'interpréter leur droit national en conformité avec ces directives mais aussi de ne pas se baser sur une interprétation de ces dernières qui entre en confit avec les droits fondamentaux précédemment mentionnés ou avec les autres principes généraux du droit communautaire, comme le principe de proportionnalité »[10]. En particulier, la Cour de Justice de l´Union Européenne a précisé: « les autorités et les juridictions nationales doivent garantir un juste équilibre entre la protection du droit de propriété intellectuelle qui protège les propriétaires du droit d'auteur et la protection de la libre entreprise, qui couvre les opérateurs, tels que les fournisseurs d'accès Internet, en vertu de l'article 16 de la Charte » [11].

Pourtant, pour Google, l'application correcte du principe de proportionnalité dans le présent litige sur le droit à l'oubli doit partir des prémisses suivantes : 1´) l'exactitude de ses référencement sur le contenu référencé des sites Web ; 2´) la mise à jour automatique et continuelle des référencements pour préserver cette exactitude de l'information ; 3´) la difficulté excessive des moyens (la suppression directe de contenus dans le référencement du moteur de recherche) qui sont prétendument utilisés pour éviter l'accès à l'information licitement publiée sur des sites Internet.

La conclusion de Google est définitive: le fait d'obliger à supprimer de son référencement des liens à des sites web serait inefficace et disproportionné pour les raisons suivantes : 1´) ce serait beaucoup moins cher et plus efficace d'obtenir le droit à l'oubli si le webmaster utilise les moyens déjà à sa disposition pour éviter les liens non seulement vers un moteur de recherche particulier mais à tous les autres, ainsi qu'à d'autres applications existantes sur Internet; 2´) parce que, avec l'intervention limitative du webmaster, les citoyens ne seraient pas contraints d'identifier la pluralité des moteurs de recherche, sites Web, réseaux, etc. dans lesquels se trouverait leur information, un seul exercice de leur droit suffirait; 3´) parce que la suppression des liens et des références dans le référencement non seulement supposerait la suppression des références

[10] Arrêt de la Cour de Justice de l'Union Européenne, 29 Janvier 2008, *Affaire Promusicae vs. Telefónica*, C-275/06.

[11] Arrêt de la Cour de Justice de l'Union Européenne, 24 Novembre 2011, *Affaire SABAM*, C-70/2010.

personnelles spécifiques mais toutes les pages Internet ce qui entraînerait progressivement une dénaturation de l'utilité du moteur de recherche et une défaillance dans son rôle central dans l'avancement de la société de l'information.

Section 2- l'AEDP défend le droit d'opposition comme droit à l'oubli dans l´état actuel de la technologie des moteurs de recherche sur internet

I-L'application de la législation espagnole au moteur de recherche de l'Internet (I): Google Espagne comme « établissement » de Google Inc en Espagne

Face au refus de Google Espagne à reconnaître la responsabilité du service de recherches, faisant valoir que ces services sont fournis par Google Inc. et que, par conséquent, ni la Directive européenne 95/46, ni aucune législation espagnole sur la protection des données est applicable du fait que Google Espagne a une activité limitée à la vente de publicité en annexe du moteur de recherche, l'AEPD a pourtant maintenu le contraire en se fondant sur les arguments suivants.

L'article 2.1 a) LOPD s´applique à tout traitement des données à caractère personnel « lorsque le traitement est effectué sur le territoire espagnol dans le cadre des activités d'un établissement du responsable du traitement », autrement dit, cette norme transpose la Directive 95/46 de protection des données qui proclame que les États membres appliquent des dispositions nationales adoptées pour l'application de la directive à l'ensemble du traitement des données personnel quand le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre.

Ainsi, le droit espagnol s'appliquerait, selon l´art. 4.1 a) de la Directive 95/46 à Google Espagne s'il était considéré comme un « établissement » dans le cadre duquel sont réalisées, sur le territoire espagnol, des activités de traitement de données du moteur de recherche. En d'autres termes, Google Espagne est-il l´établissement responsable en Espagne du traitement des données effectué par le moteur de recherché ?

La réponse à la question précédente oblige à réaliser un exercice d'interprétation qui prenne en compte les textes qui servent principalement à l'interprétation de la Directive 95/46, c'est-à-dire, les considérants qui accompagnent les préceptes qui y sont intégrés et, deuxièmement, non moins important, les avis élaborés par le Groupe de Travail intégré par toutes les Autorités de Protection des Données de l'Union Européenne créé par l'article 29 de la Directive 95/46 précisément dans ce but consultatif.

Tout d'abord, il est pertinent, pour déterminer la volonté du législateur européen sur l'application territoriale de la législation nationale pour fournir une garantie effective des droits, le considérant 18 de la directive:

« considérant qu'il est nécessaire, afin d'éviter qu'une personne soit exclue de la protection qui lui est garantie en vertu de la présente directive, que tout traitement de données à caractère personnel effectué dans la Communauté respecte la législation de l'un des États membres; que, à cet égard, il est opportun de soumettre les traitements de données effectués par toute personne opérant sous l'autorité du responsable du traitement établi dans un État membre à l'application de la législation de cet État ».

Deuxièmement, pour déterminer si dans le cas de Google Espagne nous nous trouvons devant un « établissement » au sens de l'article 4. 1 a) de la Directive, il serait crucial d'avoir recours aux dispositions du considérant 19 :

« considérant que l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable; que la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard; que, lorsqu'un même responsable est établi sur le territoire de plusieurs États membres, en particulier par le biais d'une filiale, il doit s'assurer, notamment en vue d'éviter tout contournement, que chacun des établissements remplit les obligations prévues par le droit national applicable aux activités de chacun d'eux .

Comme on peut l'observer, les deux considérants sont principalement orientés vers l'intention d'accorder une garantie effective du droit à la protection des données : d'une part, en confirmant l'exigence inéluctable que tout traitement de données effectué sur le territoire européen soit soumis à la législation d'un des États membres ; d'autre part, en évitant les formalismes qui permettent d´éviter l´application de la législation nationale par l'autorité compétente.

L'anticonformisme du considérant 19 de la Directive 95/46 permet d´attribuer le statut d'établissement à l'entité qui, par une installation stable, exerce une activité efficace et réelle, indépendamment de la forme juridique en question: succursale ou filiale dotée de la personnalité juridique. Il s'agit, sans doute, d'une approche inéluctable de la notion « d' établissement » nécessaire dans le monde actuel, complexe et hétérogène, de la société de l'information où, en particulier, les entreprises multinationales opérant sur Internet offrent les plus diverses modalités de représentation au niveau local et la plupart du temps, en tentant d´éviter l'application de la législation des pays dans lesquels elles opèrent en se soumettant à la législation américaine.

Les moteurs de recherche, loin d'être étrangers à la problématique ci-dessus, la personnifient de manière paradigmatique et pour percer le marasme juridico-formel posé par le considérant 19 de la directive, il faut avoir recours à l'Avis 1/2008, du 4 avril, sur les moteurs de recherche[12], dans lequel le Groupe de Travail de l´Article 29 a défini certains critères permettant de conclure quand il y a un « établissement » - quelle que soit sa forme juridique -:

1´) lorsqu'un moteur de recherche établit un bureau dans un État membre qui est impliqué dans la vente de publicité destinée aux habitants de cet État;
2´) lorsqu'un établissement est responsable des relations avec les utilisateurs du moteur de recherche dans une juridiction particulière;
3´) lorsqu´un établissement d'un moteur de recherche respecte les arrêts des tribunaux et/ou répond aux demandes des autorités compétentes d'un État membre par rapport aux données des utilisateurs.

L'AEPD a accumulé des éléments de preuve démontrant l'existence pour Google Espagne de ces trois critères pour déterminer sa nature comme établissement localisé en Espagne responsable pour le moteur de recherche.

---

[12] Cet avis a déclaré que la législation européenne est applicable aux moteurs de recherche et a imposé une réduction significative des périodes de rétention des données. Voir KOSTA, E., KALLONIATIS, CH., MITROU, L. ET KAVAKLI, E.: "The "Panopticon" of search engines: the response of the European data protection framework", *Digital Privacy*, Springer, vol. 16, 2010, pp. 47-54.

Premièrement, il est évident que la publicité personnalisée est le moyen de financement du moteur de recherche Google sans que l'utilisateur puisse l'éviter s´il veut utiliser le moteur de recherche et le traitement de données que réalise Google est destiné à fournir des services aux usagers parmi lesquels se trouve la publicité personnalisée. Bien sûr, la publicité liée au service de recherche et dirigée spécifiquement aux le territoire espagnol est la base de l'activité de Google Espagne. Par conséquent, l'activité économique de Google Inc. qui est réalisée dans le territoire espagnol est la génération de publicité insérée dans le service de recherche gratuit en utilisant des promoteurs locaux, tels que Google Espagne, qui font la promotion et la vente d'espaces publicitaires.

Deuxièmement, face à l'argument habituel de Google Espagne, prétendant que sa représentation en Espagne est limitée à la promotion de la vente de publicité et qu'elle n'a aucune responsabilité vis-à-vis du respect des règles de protection des données, l'AEPD illustre par de nombreuses résolutions avec des données qui mettent en évidence la représentation de Google Inc. par Google Espagne dans divers processus traités par l'AEPD. Ainsi, Google Espagne a participé à de nombreuses procédures de l'inspection de l'AEPD pour la tutelle des droits en ce qui concerne les demandes formulées par des citoyens espagnols à propos du service de recherche[13].

Troisièmement, loin de limiter son activité à la promotion de vente de publicité, Google Espagne étend sa représentation de Google Inc en Espagne à la promotion et même aux litiges sur les autres services de Google concernant la protection des données. Par exemple, la plaidoirie de Google Espagne dans le cadre de l'enquête (*expediente de actuacciones previas de inspección*) E/01544/2007 pour la plainte déposée par une organisation espagnole d'utilisateurs de la messagerie gratuite « Gmail ». Au vu des déclarations personnes de ses dirigeants, l'intervention de Google Espagne en tant que représentant de YouTube dans les médias est également notoire.

Quatrièmement, Google Inc et Google Ireland ont désigné Google Espagne, dans les déclarations du Registre Général de Protection des Données de l'AEPD, comme étant l'entité exerçant des droits d'accès, de rectification, annulation et opposition en vertu de la Loi sur la protection des données.

Tout ce qui précède conduit l'AEPD à conclure favorablement à la condition de Google Espagne comme représentant en Espagne de Google Inc., en qualité d'établissement responsable du service de recherche.

II-L'application de la loi espagnole au moteur de recherche de l'Internet (II): Google « utilise des moyens » situés en Espagne.

L'application de la législation espagnole de protection des données peut dériver, alternativement ou cumulativement, d'un second point. L'article 2.1 paragraphe c de la LOPD oblige l´application de cette loi « lorsque le responsable du traitement de données n'est pas établi sur le territoire de l'Union européenne et qu'il utilise dans le traitement des données des moyens situés en territoire espagnol, sauf lorsque ces moyens sont utilisés uniquement à des fins de transit ». Cette disposition transpose l'article 4 de la directive 95/46 de protection des données.

---

[13] TD/299/2007, TD/463/2007, TD/814/2007, TD/155/2008, TD/387/2008, TD/420/2008, TD/444/2008, TD/569/2008 et TD/580/2008.

Pour déterminer la volonté du législateur européen sur l'applicabilité territoriale de la loi espagnole aux activités des moteurs de recherche avec l'aide des moyens situés dans un État membre, il convient d'analyser le considérant 20 de la Directive:
« (20) considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'État membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés ».

Avec ce nouveau critère, la Directive 95/46 complète l'approche anti-formaliste qui préside la notion d'"établissement » avec une approche téléologique qui met en valeur les fins servies par la Directive 95/46 et qui ne peuvent pas être détournées en raison du caractère transnational des nombreux services Internet. Autrement dit, ce considérant 20 constate l'existence habituelle dans l'environnement Internet de responsables des services que se trouvent dans des pays tiers (encore une fois, principalement, les Etats Unis) et avertit que cette pratique « ne devrait pas entraver » la protection des droits individuels. Par conséquent, on réaffirme la validité de la législation de des États membres dans lesquels se trouvent des moyens pour réaliser le traitement des données et on met en garde contre « l´adaptation » des garanties prévues dans les règles de protection des données prévues par la directive. Enfin, l'approche normative-formaliste enracinée dans les catégories traditionnelles de l'articulation des responsabilités transnationales doit céder le pas à une vue matérielle et réaliste qui, dans la pratique, garantie effectivement les droits.

Cela étant dit, lorsque les services de recherche Internet utilisent des « moyens » situés dans un État membre, cela ne relève pas expressément de la Directive 95/46 et pour cela, encore une fois, le recours aux avis du Groupe de Travail de l'article 29 est d'une aide précieuse.

Concrètement, dès le 30 mai 2002, *le document de travail n° 56, relatif à l´application internationale de la législation communautaire sur la protection des données pour le traitement des données personnelles sur Internet pour les sites web établis en dehors de l'UE* a été adopté, illustrant la casuistique des « moyens » situés dans le territoire d'États membres auxquels seraient applicable l´article 4.1 c) de la Directive 95/46: « Les ordinateurs , les terminaux et les serveurs, qui peuvent être utilisés pour presque tous les types d'opérations de traitement des données, sont des exemples de 'moyens'... »

Mais, en s'inspirant du document antérieur, l'Avis 1/2008, du 4 avril, sur les moteurs de recherche, dégagera des conclusions précises quant à l'applicabilité du droit national aux moteurs de recherche Internet utilisant des moyens situés dans les États membres.
Les moyens suivants devront être considérés:

1´) les centres de données situés sur le territoire d'un État membre peuvent être utilisés pour le stockage et de traitement des données personnelles;
2´) l'utilisation des ordinateurs personnels, terminaux et serveurs;

3´) utilisation des cookies et des logiciels similaires[14].

Compte tenu de l'interprétation des critères énumérés, l'AEPD a approfondi l´analyse sur les methods par lesquelles le moteur de recherche de Google redirige ses services spécifiquement sur le territoire espagnol [15] ainsi que sur les circonstances qu´illustrent l'utilisation par le moteur de recherche des moyens en Espagne.

En Espagne, ce service de recherche est offert sur le site www.google.es. Les serveurs Web situés en Espagne sont visités par le moteur de recherche de Google pour alimenter son stock d'information et, par la suite, offrir leurs résultats, en particulier, aux utilisateurs espagnols. Les informations trouvées, stockées et référencées par le moteur de recherche depuis des serveurs situés en Espagne feront références aussi bien à des données des utilisateurs qu'à des tiers. La langue utilisée dans les documents ou sur les serveurs web qui les logent est l'élément déterminant dans l'action de recherche du moteur car, de fait, l'utilisateur décide si les résultats de sa recherche fait référence à des pages situées en Espagne. Pour offrir cette possibilité, le moteur de recherche a besoin d'accéder aux serveurs web espagnols, de stocker l'information trouvée pour les offrir à l'utilisateur situé en Espagne, tout cela logiquement, en utilisant des moyens techniques situés sur le sol espagnol.

En second lieu, l'AEPD met l'accent sur le fait que le service de recherche de google.es vise spécifiquement le territoire espagnol si l'on prend en considération les éléments suivants : 1) la langue utilisée dans google.es est l´espagnol, bien qu'il admette, même, les versions catalanes, basque et galicienne; 2) le domaine utilisé par le moteur de recherche Google en Espagne

---

[14] L'Avis nº 56 du Groupe de Travail de l´Article 29 conclut: « le PC de l'utilisateur peut être considéré comme un "moyen" en vertu de la lettre c) du paragraphe 1 de l'article 4 de la Directive 95/46/CE. Il est situé sur le territoire d'un État membre. Le responsable a décidé de l'utiliser pour le traitement des données à caractère personnel, et comme cela est expliqué dans les paragraphes antérieurs, plusieurs opérations techniques ont lieu, sans contrôle de la part de l'intéressé. Le responsable du traitement emploie les moyens de l'utilisateur et il ne le fait pas seulement dans le but de transit sur le territoire de la communauté. Le groupe de travail estime donc que les conditions dans lesquelles peuvent être recueillies des données personnelles de l'utilisateur au moyen du placement de cookies sur son disque dur sont réglementés pr le Droit national de l'Etat membre où se situe l'ordinateur personnel. »

[15] L'arrêt de la Cour de Justice de l'Union Européenne du 7 Décembre 2010 (C-585/08 et C-144/09), *Pammer vs Reederei Karl Schlüter GmbH & Co KG et Hotel Alpenhof GesmbH vs Oliver Heller*, l'illustre sur des points qui peuvent constituer des éléments de preuve qui permettent de considérer que l'activité particulière est adressée à l'État membre du domicile du consommateur avec le caractère non exhaustif: le caractère international de l'activité, l'utilisation d'une langue autre que celle normalement utilisée dans l'État membre, la mention des numéros de téléphone avec indication d'un préfixe international, l'utilisation d'un domaine de niveau supérieur de nom autre que l'État membre dans lequel il est établi le vendeur et la mention d'une clientèle internationale composée de clients domiciliés dans différents États membres. Il correspond à la juridiction nationale de vérifier s'il y a ces indications. En revanche, le simple fait que vous pouvez accéder à la page web du vendeur ou de l'intermédiaire dans l'État membre du domicile du consommateur est insuffisant. Le même phénomène se produit avec la mention d'une adresse de messagerie et d'autres données ou l'utilisation d'une langue couramment utilisée dans l'État membre dans lequel le fournisseur est établi.

(google.es) est un domaine territorial immatriculé dans Red.es correspondant au code pays Espagne; 3) les résultats indexés dans google.es s´adressent essentiellement aux utilisateurs situés sur le territoire espagnol. 4) Google est financé par la publicité jointe aux résultats de recherche qui démontrent ses liens spécifiques pour le territoire espagnol.

III-L'application de la loi espagnole au moteur de recherche Google (III): Loi de Services de la Société de l'Information et Directive 2000/31

Le débat récurrent sur l'application de la législation de la protection des données aux services de recherche sur Internet des sociétés situées en dehors de l'Union européenne ignore quelquefois l'existence de lois spécifiques ciblant ces services de la société de l'information qui ne laissent aucune place au doute sur l'application de la législation nationale et spécifiquement espagnole.

Ainsi, la Loi 34/2002, du 11 juillet, des Services de la Société de l'Information et du Commerce Électronique (LSSI) – qui transpose la Directive 2000/31 sur le commerce électronique dans le marché intérieur - établit dans son article 4 que les services dirigés spécifiquement au territoire espagnol – ce qui, pour l'AEPD, serait le cas du moteur de recherche Google, seront – « soumis aux obligations prévues par la présente loi, sous réserve que cela ne contrevienne pas aux dispositions des traités ou conventions internationales applicables ». En particulier, l'article 8,1 c) LSSI ajoute: « dans le cas où un service particulier de la société de l'information soit susceptible de menacer le respect de la dignité de la personne, les organes compétents pour leur protection, dans l'exercice de leurs fonctions qui leurs sont attribuées légalement, peuvent prendre les mesures nécessaires afin d'interrompre sa prestation ou pour supprimer les données qui les violent ».

Loin, donc, de protéger l'impunité des moteurs de recherche d´Internet, la LSSI les soumet aux obligations prévues dans la norme lorsque qu'ils dirigent leurs services au territoire espagnol et prévoit la possibilité que les autorités compétentes peuvent interrompre ses services ou retirer ces données illégales en violation du respect de la dignité humaine. L'AEPD s´attribue le statut d'autorité nationale habilité par la législation espagnole pour décider de l'interruption de service de la société de l'information ou de la suppression des données qui violent le respect à la dignité humaine et, par conséquent, les droits fondamentaux (art. 10.1 de la Constitution Espagnole), parmi lesquels le droit à la protection des données personnelles qui est ici concerné au plus haut point .

En particulier, les nombreuses résolutions de l'AEPD réaffirment le lien entre la dignité humaine et la protection des données : « l´article 18.4 de la Constitution espagnole contient... un droit ou liberté fondamentale, le droit à la liberté contre les potentiels attaques à la dignité et la liberté de la personne par l´usage illégitime du traitement automatisé de données, ce que la Constitution appelle 'l´informatique'... le droit fondamental à la protection des données a pour but de garantir un contrôle sur les données personnelles afin d'éviter leur trafic illicite et des dommages à la dignité et les droits des personnes » (arrêt de la Cour Constitutionnelle 292/2000).

IV- La responsabilité de Google après la « connaissance effective » de l'illégalité des recherches

La Directive 2000/31 du 8 juin 2000 sur le commerce électronique déclare, en général, l'absence d'une obligation générale de surveillance dans son article 15.1 : « Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une

obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ».

Toutefois, en transposant l´article 14 de la Directiva 2000/31, la LSSI réglemente dans son article 17 « la responsabilité des prestataires qui fournissent des liens aux contenus et des outils de recherche »:

1) En règle générale, l'article 17 LSSI exonère de toute responsabilité « les prestataires de services de la société de l'information qui facilitent des liens vers d'autres contenus, ou qui incluent dans ses répertoires ou instruments de recherche de contenu » pour les données qu'ils diffusent (en définitive et en général, cela concerne les moteurs de recherche pour la diffusion de données d'internet et en particulier à Google Search.)

2) Toutefois, la responsabilité du moteur de recherche des résultats de la recherche du émerge lorsque deux conditions sont réunies:

a) une connaissance effective par le moteur de recherche de l´illégalité de l'information; b) une non-action avec la diligence nécessaire pour la supprimer ou désactiver le lien.

Les moteurs de recherche d´Internet, en tant que services d'intermédiation qui n'offrent pas des contenus propres, n´ont *a priori* [16] aucune responsabilité sur les contenus qu'ils trouvent, stockent, référencent et diffusent en ligne. Ainsi, le traitement automatisé des moteurs de recherche ne génère pas de responsabilité *per se* jusqu'au moment où la neutralité de l'opérateur cède à la connaissance et les lois obligent à préserver la garantie des droits fondamentaux[17].

La responsabilité du moteur de recherche émerge, par conséquent, lorsque se produisent trois conditions: 1) « déclaration de l'illégalité de l'information », 2) « connaissance effective »; 3) et « manque de diligence raisonnable » pour la suppression.

L´article 17 LSSI fournit également deux éléments supplémentaires pour préciser ces exigences:

1) établir la « connaissance » au moment où le fournisseur de service a connu la résolution de l'organe compétent qui déclare l'illégalité des données et ordonne la suppression;

2) rien n'empêche que le fournisseur de services acquière une connaissance effective en appliquant leurs accords volontaires de détection et de suppression de contenu.

---

[16] Il est intéressant de noter que la Cour de Justice de l'Union Européenne, (C-70/2010, arrêt du 24 novembre 2011) *Affaire SABAM*, après un examen conjoint des directives 2000/31, 2001/29 et 2004/48, rejete de forcer à certains services de la société de l'information à un filtrage "indiscriminé et préventif" du contenu.

[17] L´Arrêt de la Cour de Justice de l'Union Européenne, 23 mars 2010 (C-236/08 et C-238/08), Google France vs Louis Vuitton, dit: "les exonérations de responsabilité établies dans la Directive 2000/31 ne s'applique qu'aux cas où l'activité du prestataire des services aient « un caractère purement technique, automatique et passif », ce qui implique que le prestateur n'a aucune connaissance ou contrôle des informations transmises ou stockées". Par conséquent, pour vérifier si la responsabilité de fournisseur de service de référencement pourrait être limitée conformément à l'article 14 de la Directive 2000/31, il est nécessaire d'examiner si le rôle joué par le fournisseur est neutre, c'est-à-dire, si leur comportement est purement technique, automatique et passif, ce qui signifie qu'il n'a aucune connaissance ou contrôle de l'information stockée.

Ainsi, les exigences légales pour demander la responsabilité juridique (civile, pénale ou administrative, conformément à l'article 13 LSSI) du moteur de recherche Google pour référencement et diffusion de données illicites semblent, à première vue, diaphanes.

V-La responsabilité de Google, partagée avec le webmaster, comme un corollaire de l'impact des moteurs de recherche d´Internet

La modalité de répartition des responsabilités entre des sites Web et moteurs de recherche d´Internet relatif aux informations référencées n'est pas aussi simple qu'elle en a l'air. En l'absence de référence précise dans la Directive 95/46 et dans la LOPD sur comment appliquer aux moteurs de recherche les droits et obligations découlant des normes de protection des données, il est essentiel recourir à des principes généraux.

L´Avis 1/2008 du Groupe de Travail de l'article 29, sur le principe de responsabilité, fait la différence entre responsabilité principale (moteurs de recherche) et secondaire (webmaster).

Autrement dit, même si parfois semble acquise l´idée intéressée selon laquelle la responsabilité sur Internet est exclusivement imputable aux webmasters tandis que les moteurs de recherche jouissent d'une sorte d'impunité/irresponsabilité dérivée de leur prétendue neutralité, il n'y a rien de plus éloigné de la réalité, compte tenu de l'interprétation de la Directive 95/46 prévu par le Groupe de Travail de l'article 29.

Il est vrai qu´une application correcte du principe de proportionnalité exige d'examiner que les moteurs de recherche agissent uniquement en tant qu'intermédiaires et, par conséquent, ils ne peuvent pas être considérés responsables principaux du traitement ou de la publication sur Internet de telles informations. Surtout lorsque les webmasters sont en conditions d'éviter, à travers les robots.txt et les balises Noindex/no archive, la capture de ces informations par les moteurs de recherche. Mais, cela n'exclut pas la responsabilité du moteur de recherche qui émerge a posteriori lorsqu'on s'interroge sur sa légalité à contrevenir aux les règles de protection des données: « La responsabilité formelle, juridique et pratique du moteur de recherche est généralement limitée à la possibilité de supprimer les données de vos serveurs. Pour ce qui se réfère à la suppression des données personnelles de son référencement et ses résultats de recherche, les moteurs de recherche ont une responsabilité suffisante pour être tenu responsable pour le traitement (seul ou conjointement avec d'autres) dans ces cas ».

Par conséquent, Google participe à une « responsabilité suffisante » qui le forcera à intervenir lorsque la suppression des données personnelles de son référencement et du résultat de la recherche est exigée. Aussi, les moteurs de recherche porteront « pleine responsabilité » dans de nombreux cas, quand ils ne sont pas limités à agir comme de simples intermédiaires, (a) recueillant des données à caractère personnel auprès des serveurs de l'Internet, (b) ou orientant l'exploration, l'analyse et l'indexation à l'aide des informations identifiables personnellement (comme cela peut se produire avec la reconnaissance faciale).

Dans la société de l'information, les services offerts sur Internet ont une telle complexité et génèrent un tel impact sur la protection des données que, loin d'admettre l'absolue impunité, il n'est pas difficile d'imaginer une graduation dans la responsabilité des moteurs de recherche comme « responsabilité principale », « responsabilité partagée », « responsabilité pleine » ou « responsabilité suffisante ».

Par conséquent, comme le rappelle l'Avis 1/2008, l'obligation de suppression des données personnelles de l'index de recherche constituera une responsabilité des moteurs de recherche dans la mesure où l'obligation de retirer ou de bloquer les données à caractère personnel peut dépendre de la législation sur la responsabilité civile et de normes dans le domaine de la responsabilité de l'État membre[18].

VI-Le droit d'opposition comme instrument équilibré pour un exercice réactif – ni prévention, ni filtrage, ni censure - du droit à l'oubli

Les droits à la protection des données s´appliquent à l'activité des moteurs de recherche. De nouveau, l'apparente neutralité générée par l'activité informatisée d'intermédiaire des moteurs de recherche n'a pas empêché l'Avis 1/2008 de proclamer l´applicabilité des droits à la protection des données aux les moteurs de recherche. Une question fort différente, compte tenu de la diversité de ce phénomène technologique, sera la force et la viabilité de ces droits selon les différentes activités que génèrent les moteurs de recherche et selon la nature diverse des sujets concernés. La situation des individus est différente selon si les utilisateurs sont authentifiés et avec des profils personnels, non enregistrés ou même des tiers dont les données personnelles sont hébergées sur des sites Web et indexées par les moteurs de recherche. La situation des renseignements personnels contenus dans les profils personnels enregistrés, dans les caches de mémoire ou dans les index du moteur de recherche est également différente.

Explicitement, l'Avis 1/2008 fit référence au le droit à demander la suppression de données par les moteurs de recherche dans les termes suivants : 1) les moteurs de recherche devraient respecter le droit de supprimer des données - en particulier, des utilisateurs authentifiés et de leurs profils personnels mais, également, des non inscrits-; 2) un droit identique s'applique aux données de caches mémoire qui doivent être supprimées rapidement si elle sont « incomplètes ou obsolètes », c'est-à-dire « une fois que ces données ne correspondent pas au contenu publié sur Internet »; 3) aux fins susmentionnées, les moteurs de recherche doivent mettre à jour automatiquement la publication originale; 4) les webmasters devraient prendre des mesures pour informer automatiquement les moteurs de recherche de toutes les demandes de suppression des données reçues.

Mais, le droit à l'oubli sur Internet prend en charge son exercice par le biais de deux instruments juridiques qui, bien que d'apparence semblable et de résultat identique, ont une portée très différente sur Internet et, en particulier, sur l'activité de leurs moteurs de recherche: le droit de « suppression » et le « droit d'opposition ».

Le droit de suppression prévu à l'article 16 LOPD prévoit que le contrôleur est tenu de rendre efficace le droit de suppression lorsque le traitement des données n'est pas conforme aux dispositions de la présente loi et, notamment, lorsque ces données sont inexactes ou

---

[18]Comme nous l'avons mentionné précédemment, l'Avis 1/2008 mentionne expressément le cas de l'Espagne quand il signale que, « dans certains États membres de l'UE autorités de protection des données ont réglementé spécifiquement l'obligation des fournisseurs de supprimer le contenu du référencement de recherche, sur la base du droit d'opposition consacré par l'article 14 de la Directive sur la protection des données (95/46/CE) et de la Directive sur le commerce électronique (2000/31/CE). En vertu de ces lois, les moteurs de recherche sont obligés de suivre une politique de notification et de suppression semblable à celle suivie par les fournisseurs de services d'hébergement, afin d'éviter la responsabilité ».

incomplètes[19]. Comme il est évident, appliquer directement cet article sur Internet et, en particulier, à l'activité des moteurs de recherche est très controversé car, l'inexactitude, le caractère incomplet ou l'inexistence d'une autorisation pour le traitement des données impliquent une faculté permettant à tout utilisateur qui pourrait mettre en question la nature et l'utilité des recherchés comme des outils essentiels de la société de l'information.

Toutefois, le *droit d'opposition* permet des objectifs identiques (suppression de données personnelles référencées) mais par des moyens plus conformes au principe de proportionnalité dans la mesure où la suppression de données exige une pondération individualisée des raisons qui la justifient et ne couvre donc pas une autorisation générique de la suppression d'information sur Internet. Et il en est ainsi parce que l'article 6.4 LOPD prévoit que, dans le cas où le consentement des personnes n'est pas nécessaire et une loi ne l´impose pas, on pourra s'opposer au traitement lorsqu'il existe des *motifs légitimes et fondées relatifs à une situation personnelle particulière*[20].

Par conséquent, pour l'AEPD, le droit d'opposition sur renseignements personnels indexés par les moteurs de recherche d'Internet - comme outil optimal pour garantir le droit à l'oubli – se fonderait sur des prémisses sociologiques et juridiques suivantes:

L'absence de filtrage préventif des données par des instruments techniques qui pourraient s'apparenter à de la censure;

L'absence de toute loi qui oblige l´hébergement des données sur des sites Internet, référencement ou mémoire cachée des moteurs de recherche;

L'invocation individuelle de raisons bien fondées et légitimes concernant une situation personnelle à travers une procédure réactive;

Le manque d'intérêt public dans les données personnelles publiées sur Internet.

Comme il a été proclamé par l'AEPD, les effets extraordinaires multiplicateurs qu´aujourd'hui provoquent, lors de la diffusion de renseignements personnels, les moteurs de recherche d´Internet comme instrument de communication universelle que préserve sa maintenance globale, obligent à l´existence des instruments efficaces qui permettent de préserver le droit à l'oubli pour éviter les dommages sur la dignité humaine liés à l'évolution de la société de l'information.

L'existence d'un mécanisme juridique permettant à l'individu de réagir aux données à caractère personnel qui sont hébergées sur les index des moteurs de recherche, faisant valoir des circonstances personnelles légitimes que protègent leur suppression, ne peut pas être estimée comme attentatoire au du rôle social indéniable joué par les moteurs de recherche d´Internet.

---

[19] Cet article transpose l'article 12 de la Directive 95/46: « Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement (...) la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données ».

[20] L'article 14 de la Directive 95/46, que cet article transpose, établit: « Les États membres reconnaissent à la personne concernée le droit de (...) s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national. »

VII-Le droit à l'oubli sur les moteurs de recherche dans l'état actuel du développement technologique : limitations techniques

Ce qui précède n'empêche pas, toutefois, à reconnaître la faiblesse du critère résolutoire de l'AEPD devant les difficultés techniques qu'apparemment déclenchent la mise en application des résolutions qui garantissent le droit à l'oubli dans les moteurs de recherche « exhortant à prendre les mesures nécessaires pour supprimer les données personnelles du référencement de recherche et à empêcher son accès futur ».

Supprimer un lien du résultat de la recherche en appréciant des raisons bien fondées et légitimes relatives à une situation personnelle particulière ne devrait pas poser plus de difficultés techniques au moteur de recherche - après le traitement de la réclamation individuelle ou de la résolution de l'Autorité de protection de données compétente.

Au contraire, l'AEPD exige, aussi, pour garantir le droit à l'oubli, que les moteurs de recherche d´Internet « adoptent les mesures nécessaires pour empêcher l'accès futur aux données » figurant dans les liens de l'index. Et voici où les allégations de Google acquièrent une valeur qui ne peut pas être banalisée : sans l'intervention du webmaster (avec l'aide du fichier *robots.txt* ou des balises *Noindex/ non archive*) pour limiter l'accès futur à son contenu, le moteur de recherche continuera à référencer et à diffuser des données personnelles qui ont été retirées de l'index en admettant le droit d'opposition.

La vérité est que, actuellement, la prétendue impossibilité technique pour empêcher l'accès futur des moteurs de recherche aux données existantes sur Internet (à moins que le webmaster collabore) est un lieu commun, accepté par l'industrie de l'Internet et apparemment par toute la communauté technologique. Toutefois, cette prémisse n'a jamais été testé par ceux qui seraient en mesure de le faire (l'industrie même des moteurs de recherche d´Internet) et rien n'empêche d'imaginer (à la lumière de l´évolution extraordinaire dans les services Internet) que les développements technologiques permettent d'arbitrer des mécanismes techniques pour assurer ce droit à l'oubli.

Mais, si un règlement ou une décision administrative oblige à « empêcher l'accès futur » et le moteur de recherche n´est pas en mesure de prouver son infaisabilité technique, quels sont les effets juridiques de ces actes? L'impossibilité de la mise en œuvre de la résolution est à l'origine d'une certaine impunité pour le moteur de recherche, ou ce dernier méritera-t-il reproche ou sanction?[21].

Les choses ne sont pas toujours nécessairement ce qu'elles paraissent. L´AEPD demande à Google « d'adopter les mesures nécessaires pour empêcher l'accès futur » aux données supprimées du référencement de recherche. L'unique responsable de la suppression des données du référencement de recherche est, sans aucun doute, Google. Mais « prendre des mesures pour empêcher l'accès futur aux données » ne signifie pas nécessairement et exclusivement obliger Google tout seul à éviter techniquement de nouveaux référencements.

---

[21] Voir la très intéressante analyse faite par v. mayer-schönberger sur la possibilité de mettre en œuvre sa proposition visant à introduire les dates d'expiration de données aux résultats de recherche des moteurs de recherche (*Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Oxford, 2009, pp. 179-180).

L'AEPD a opté pour une formule assez flexible pour adapter l'obligation normative au développement de la technologie:

a)Quand les résolutions de l'AEPD exhortent Google à « adopter les mesures nécessaires pour empêcher l'accès futur aux données personnelles », cela laisse peut de marge à l'interprétation : l'AEPD lui *ordonne* d'empêcher directement (sans la collaboration du webmaster) le futur référencement selon les possibilités offertes par l'état actuel du développement de la technologie des moteurs de recherche d´Internet et en même temps, elle l'*invite* à perfectionner sa technologie pour rendre possible ces mesures [22].

b)Mais, tant qu'il n'y a aucune technique permettant au moteur de recherche d´empêcher directement (nécessitant, par conséquent, la collaboration du webmaster) le nouveau référencement des liens déjà précédemment supprimés du référencement, les « mesures nécessaires » à adopter par Google sont satisfaites par la technologie que le moteur de recherche offre aux webmasters pour limiter l'accès à son contenu.

Toutefois, il est difficile d'admettre l'allégation de Google sur l'impossibilité technique d'éviter l'accès futur aux résultats de recherche si on prend en compte sa *Politique de la Vie Privée* concernant la façon de *supprimer le contenu du site d´un autre utilisateur* [23], même lorsque le webmaster ne le supprime pas ou n´empêche pas son référencement. [24].

De fait, en suivant le protocole de Google pour supprimer les résultats de recherche autant du Web que du référencement, si le requérant a été en contact avec le webmaster, mais, par exemple, n'a pas reçu de réponse, Google reconnaît au demandeur « qu´il est possible de vous aider » [25]

---

[22] Cette approche suit la thèse maintenue par J. R. REIDEMBERG selon laquelle la solution aux problèmes de la protection des droits sur l'Internet doit provenir de «l´innovation» dans les technologies de l'information: "the assertion of sovereign jurisdiction to protect citizens is likely to advance the fundamental public policy that the rule of law should be supreme to technological determinism. At the same time, the multiplicity of states with jurisdiction over Internet activities is likely to stimulate creativity and new Internet services such as more accurate and selective filtering technologies, stronger security zones and more robust, customized compliance capabilities" ("Technology and Internet Jurisdiction"..., p. 1974).

[23] http://support.google.com/webmasters/bin/answer.py?hl=es&answer=1663688

[24] « Nous supprimons le contenu dans très peu de résultats de la recherche de manière discrétionnaire. En plus du spam, nous prenons seulement des mesures avec un certain type de données à caractère personnel (précisez ci-dessous) et le spam "pour adultes". Si un utilisateur nous le demande, nous allons supprimer les informations personnelles si nous pensons qu'il pourrait lui porter préjudice en quelque sorte en particulier, comme en cas de vol d'identité ou de fraude financière. Parmi ce type d'information, notamment des numéros d'identification nationaux confidentiels, comme la sécurité sociale, compte bancaire ou cartes de crédit, ainsi que des images de signatures. Cela n'inclut pas des données comme la date de naissance, l'adresse ou le numéro de téléphone de l'utilisateur (...) Pour déterminer si un type particulier d'information est considérée comme confidentiel, nous appliquons des critères tels que les suivants: Est-ce un numéro d'identification émis par le gouvernement? Relève-t-il d'une information privé ou du domaine public? Peut-il être utilisé pour effectuer certaines opérations financières courantes? Peut-il être utilisé pour obtenir plus d'informations sur une personne? Nous appliquons cette politique de suppression de contenu en fonction des particularités dans chaque cas. Parfois, nous rejetons les demandes si nous croyons que quelqu'un essaye de faire un usage inapproprié de ces stratégies pour supprimer les informations de nos résultats. Nous allons supprimer n'importe quelle page qui contient le spam avec un contenu sexuel explicite et le nom complet d'un utilisateur ou de votre entreprise si nous recevons une demande » Traduction de la page en espagnol.
https://support.google.com/websearch/answer/2744324

[25]https://support.google.com/websearch/troubleshooter/1209905#ts=1231445,2889054,2889099,2889064

lorsque les données concernées sont des numéros de compte bancaire ou de carte de crédit, l'image de la signature manuscrite, du contenu pornographique qui inclut un nom complet, etc. C'est-à-dire qu'il y a une reconnaissance explicite par Google de ses possibilités techniques pour la suppression des liens du référencement du moteur de recherche.

VIII-Critères spécifiques pour les médias en ligne: pondération entre le préférentiel droit à l'information et la demande légitime de l'oubli

Une analyse juridique du conflit entre les droits à l'information et protection des données doit partir inévitablement de la transcendance que le premier a dans les sociétés démocratiques et de la nécessité de résoudre le conflit selon les bases juridiques suivantes:

1) Il n'y a pas de démocratie sans élections libres, et celles-ci ne peuvent exister sans que les citoyens puissent former librement leur opinion en exerçant la liberté d'expression et le droit à l'information. Ce sont des libertés qui, au-delà de leur nature comme droits subjectifs, ont une valeur institutionnelle indispensable dans le système démocratique. Pour cette raison, toute déclaration constitutionnelle des droits a proclamé, au cours des derniers siècles, ces libertés dans des termes similaires à l'actuel article 20.1 de la Constitution espagnole: « Nous reconnaissons et protégeons les droits (...) a) d´exprimer et de diffuser librement des pensées, des idées et des opinions par la parole, par écrit ou d´autres moyens de reproduction (...) d) de communiquer ou de recevoir librement une information véridique par tout moyen de diffusion ».

2) Mais, dans le système constitutionnel il n´y a pas des droits et libertés absolus comme l´article 20.4 de la Constitution Espagnole le prouve quand elle proclame que les droits antérieurs ont leurs limites dans le respect des droits reconnus par la Constitution « et, surtout, dans le droit à l´honneur, à la vie privée et à l'image ». C'est-à-dire qu'il y a des droits constitutionnels *réévalués* lorsqu'ils sont confrontés avec les libertés de l'information (d'une part, parce qu'ils touchent la sphère personnelle de l'individu et, d'autre part, parce qu'ils peuvent menacer de manière très frappante les libertés d'expression et d'information). Et à ce groupe particulièrement qualifié de « droits limites » appartient le droit à la protection des données par volonté implicite, mais sans équivoque, de la jurisprudence constitutionnelle qui l'a consacré comme un droit fondamental (STC292/2000). Cependant, cette reconnaissance constitutionnelle récente n´évitera pas des décennies et des siècles de tradition dans la protection de l'honneur ou de la vie privée et, en pratique, sa force exécutoire sera notamment plus affaiblie que dans ces autres cas quand ils entrent en conflit avec les libertés d'information.

3) Résultant, a priori et en apparence, équivalent à son potentiel constitutionnel, comment faire pour résoudre les conflits inévitables quand entrent en conflit les libertés d'information et les droits fondamentaux concernés (et, notamment, de protection des données)? Sans aucun doute, la jurisprudence constitutionnelle a donné la prévalence aux libertés d´information[26] et donc, autrement dit, les informations véridiques sur des questions d'intérêt public sacrifient le droit fondamental à la protection des données.

---

[26] « Compte tenu de sa fonction institutionnelle, lorsqu'il y a une collision de la liberté d'information avec le droit à la vie privée et à l'honneur, elle a, en général, une position préférentielle » (STC 171/1990).

4) Cependant, cette réponse traditionnelle au conflit a, aujourd'hui, un impact sans précédent dans la société moderne de l'information et des medias[27], tout particulièrement avec l'existence de services d´Internet, tels que les moteurs de recherche, qui démultiplient les effets diffuseurs de toute information. Si la Constitution espagnole adoptée en 1978 était déjà préoccupée par les effets de l'utilisation des ordinateurs par rapport aux droits et libertés (art. 18,4 CE), en appréciant les risques d'une technologie dont la signification actuelle était inimaginable alors, il semble indéniable que ce mandat constitutionnel exige inexorablement à « réévaluer » le droit à la protection des données comme garantie spécifique et adapté (STC 292/2000) dans la société de l'information structurée autour d'Internet.

5) La résolution de l'AEPD 266/2007 a avancé un critère – mais il n'est pas suffisant - pour résoudre le conflit entre la protection des données sur Internet et les libertés d'information[28]. La Constitution protège la liberté d'information « par tout moyen de diffusion » (art. 20,1 d) CE) - Internet est certainement son expression la plus paradigmatique- et la jurisprudence constitutionnelle interdit le privilège ou « droit fondamental renforcé » pour les journalistes ou les médias (STC 225/2002). Pour cela il sera indispensable un jugement dans la publication des données personnelles sur Internet qui pondère le degré d'intérêt social ou d'utilité publique d'une information personnelle en fonction du canal de diffusion utilisé pour transmettre : web, moteur de recherche, medias de communication el ligne…etc.

6) Il convient de noter que la Directive 95/46 attribue aux Etats le pouvoir d'établir des exemptions et des exceptions aux règles de protection des données dans la mesure qu´il soit nécessaire pour concilier le droit à la vie privée et la liberté d'expression dans le traitement exclusivement journalistique de données (art. 9). En outre, son considérant 37 insiste sur le fait qu'il fallait prévoir des exceptions ou restrictions s'ils sont nécessaires pour concilier les droits fondamentaux de la personne avec « la liberté d'expression » et, en particulier, la liberté de recevoir ou de communiquer des « informations », comme garantie par l'article 10 CEDH. Le mandat est donc clair: non seulement rechercher un équilibre par la pondération - et, à défaut, sacrifier le droit à la protection des données au profit du droit préférentiel à l'information – mais aussi « concilier » les deux droits autant que possible ou, au moins, minimiser le sacrifice de l'un pour l'autre.

---

[27]Une manifestation particulière de cette réalité conflictuelle: RALLO, A. et MARTINEZ, R.: « Data Protection, Social Networks, and Online Mass Media », *European Data Protection: Coming of Age*, Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet Editors, ed. Springer, London-New York, 2013, págs. 407-430.

[28] « Aucun citoyen qui jouit ni du statut de personnalité publique ni fait l'objet d'un événement digne d'intérêt public doit se résigner à faire face à la circulation de ses données personnelles sur Internet sans pouvoir réagir ou corriger l'inscription illégale de ces dernières sur un système de communication universel comme Internet. Si le consentement individuel des citoyens est nécessaire pour inclure leurs données personnelles sur Internet ou pour exiger des mécanismes techniques qui empêcheraient ou filtrerait l'inclusion non consentie, cela pourrait supposer une infranchissable barrière au libre exercice des libertés d'expression et d'information à la manière d'une censure préalable (ce qui est constitutionnellement proscrit). Il n'en ai pas moins vrai qu'il est tout à fait légitime que le citoyen qui n'est pas obligé à se soumettre à la discipline de l'exercice des liberté susmentionnée (ses données personnelles n'étant pas du domaine public elles ne contribuent donc pas à se forger une opinion publique libre comme pilier basique de l'Etat démocratique) doit jouir de mécanismes réactifs basés sur le droit (comme le droit de suppression des données à caractère personnel), qui empêche la maintenance séculaire et universelle sur internet de son information à caractère personnel ».

7) Avec le défi de réaliser cette conciliation sans sacrifier la liberté d'information, l'AEPD proclame que « le développement de l'internet et la généralisation des moteurs de recherche » oblige à recommander aux médias en ligne de suivre les techniques et la procédure suivantes: 1) évaluer la nécessité de concilier la liberté de l'information avec l'application des principes de protection des données; 2) évaluer scrupuleusement l'intérêt public de l'identité des personnes; 3) dans le cas où l'identité des personnes ne contribue pas à offrir des informations supplémentaires, éviter l'identification par la suppression du nom et, le cas échéant, de l'initiale et toute référence complémentaire d´identification; 4) réflechir sur la conservation et l'accessibilité permanente aux données contenues dans des nouvelles journalistiques dont la pertinence est probablement inexistante aujourd'hui; 5) utiliser des mesures techniques - par exemple, les fichiers « *robots.txt* » - pour d'éviter le référencement des données par les moteurs de recherche mais sans altérer les archives journalistiques.

8) Cependant, les moteurs de recherche d´Internet n'ont pas une protection juridique spécifique pour publier les renseignements personnels et les intégrer dans leur référencement de recherche ou les garder temporairement dans le mémoire "caché". Autrement dit, il ne serait possible de parler de liberté d'information qu'à propos de ceux qui publient des nouvelles avec des données personnelles et non pas à propos des moteurs de recherche d´Internet.

9) Loin de permettre une sorte de censure général [29] préventive ou réactive ou une revendication de l'oubli générique, les limites à l'activité informative des médias en ligne ou aux moteurs de recherche d´Internet pourraient être soutenues seulement par l'existence d'une situation personnelle légitime qui permet l'exercice du droit d'opposition visé à l'article 6.4 LOPD. Et, en particulier, l'AEPD a fondé ce droit: 1) sur l'inexactitude de l'information; 2) ou sur la perte d´intérêt informatif pour cause de devenir obsolet à cause du passage du temps.

---

[29] Et, comme on peut le voir, les critères ci-dessus sont entièrement conformes aux paramètres proposés par F. DE LA RUE pour considérer légitime une restriction de contenu sur Internet: "As with offline content, when a restriction is imposed as an exceptional measure on online content, it must pass a three-part, cumulative test: (1) it must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); (2) it must pursue one of the purposes set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights , namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and (3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality). In addition, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory. There should also be adequate safeguards against abuse,including the possibility of challenge and remedy against its abusive application" (*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Assemblée générale de Nations Unies, 16 mai 2011, p. 19).

Annexe 3 :

Tableau de synthèse des résultats obtenus par l'étude des chartes et l'analyse des entretiens

Ce qui est dit dans les chartes	Ce qui est fait dans la pratique…	… et les difficultés perçues		Analyse
Définir le droit à l'oubli numérique				
Protéger les données à caractère personnel	La protection des données à caractère personnel est un élément fondamental pour les entreprises publiques à l'égard des utilisateurs. Cette protection est moins mise en avant par les entreprises privées qui accordant donnent la priorité aux données propre à leur activité, pour prendre en compte le risque d'une mauvaise image de marque si les données venaient à être divulguées aux mauvais destinataires	✔		Une finalité commune de protection des données à caractère personnel avec pour les entreprises privées la nécessité de prendre également en compte les risques d'image afférents à une mauvaise gestion des données (notamment des clients).
Non évoqué dans les chartes	Le droit à l'oubli numérique n'existe pas en tant que tel mais les pratiques respectent la loi Informatique et Liberté de 1978 et la réglementation de la CNIL sur la protection des données à caractère personnel	✔		La notion de droit à l'oubli numérique n'existe pas dans les chartes, elle n'existe pas non plus dans les pratiques. Par contre, en respectant la loi Informatique et Liberté, les entreprises respectent partiellement le droit à l'oubli numérique.
Non évoqué dans les chartes		✘	Comment respecter des règles internationales divergentes ?	Il existe une difficulté majeure lorsque les données concernées par le droit à l'oubli numérique se situent à l'étranger ou sont transférées dans des pays étrangers.

Ce qui est dit dans les chartes	Ce qui est fait dans la pratique…		… et les difficultés perçues	Analyse
Sécuriser et garantir la confidentialité des données à caractère personnel				
Mettre en œuvre les moyens techniques (mots de passe, logiciel de protection, audit, contrôle de l'usage d'internet)	La faisabilité technique du droit à l'oubli numérique est possible mais elle est difficile.	k ✘	Le problème n'est pas technique mais d'ordre soit financier (un coût parfois trop élevé) soit organisationnel (mise en place de règles complexes et difficiles à contrôler)	Les obstacles à la mise en œuvre d'un droit à l'oubli numérique ne sont pas techniques. Ils relèvent plus d'une volonté d'engager des ressources organisationnelles et budgétaires.
Allouer les ressources humaines nécessaires (les correspondants CIL ou responsables de site)	Les entretiens ont tous été réalisés avec des CIL ou des correspondants de site	✓		Les entreprises sont en conformité avec les préconisations de la CNIL en allouant des ressources humaines. Toutefois, on peut s'interroger sur la capacité de ses ressources à mener à bien leurs tâches quand les entreprises n'engagent pas les ressources budgétaires et organisationnelles nécessaires pour opérationnaliser le droit à l'oubli numérique ?
Responsabiliser les utilisateurs	Les entreprises mettent principalement l'accent sur la nécessité de sensibiliser et former les utilisateurs à respecter la sécurité des données	✓		La mise en œuvre d'un droit à l'oubli ne peut pas être exclusivement régie par des textes de loi. Le comportement des utilisateurs et donc leur sensibilisation et formation est une des clés de voûte d'un futur droit à l'oubli numérique.

Ce qui est dit dans les chartes	Ce qui est fait dans la pratique…	… et les difficultés perçues	Analyse
Sécuriser et garantir la confidentialité des données à caractère personnel			
Interdire l'accès et la divulgation des données à caractère personnel privé.	Les entreprises n'ont pas mentionné faire la différence entre données professionnelles et données à caractère privé.	Comment supprimer les données à caractère personnel qui sont devenues des données publiques ?	Le droit à l'oubli numérique suppose de gérer à la fois les données à caractère personnel et à caractère privé mais aussi leur transformation en données publiques le cas échéant
		Comment garder le contrôle des données externes (présentes sur les réseaux sociaux, les *cloud*)	Dès qu'une donnée sort de l'entreprise, sa maîtrise et son contrôle sont impossibles. Le droit à l'oubli numérique apparaît dès lors impossible à mettre en œuvre
Droits et devoirs			
Informer les utilisateurs sur le traitement des données.	Les entreprises déclarent respecter leur obligation d'information.	Comment s'assurer que chaque fichier et chaque traitement fait bien l'objet d'une déclaration ?	Les entreprises cherchent à respecter leur obligation de déclaration des traitements. Mais elles ont bien conscience qu'elles ne le respectent pas complétement. Nombres de fichiers à usage interne ne sont pas déclarés. Dès lors une question importante se pose sur la faisabilité du droit à l'oubli numérique : Comment oublier ce qui n'a pas d'existence officielle ?

Ce qui est dit dans les chartes	Ce qui est fait dans la pratique...		... et les difficultés perçues	Analyse
Droits et devoirs				
Permettre aux utilisateurs de modifier et supprimer leurs données à caractère personnel	Les entreprises s'astreignent à répondre à toute demande de modification ou de suppression des données.	✖	Comment répondre à des demandes multiples avec des ressources limitées	Si répondre aux demandes de modifications et de suppression est un droit auquel les entreprises répondent, ce droit pourrait avoir des effets délétères et des conséquences dangereuses s'il était utilisé comme une arme de déstabilisation économique
Détruire les données lorsqu'elles n'ont plus lieu d'être gardées par l'organisation	Les entreprises ne s'assurent jamais que les données ont été réellement supprimées à leur date d'expiration.	✖	Comment aussi effacer les traces numériques sur un ordinateur ou sur Internet ?	La destruction des données est difficile et dans le même temps n'est pas suffisante. Détruire les données devrait consister d'une part à faire disparaître la donnée mais également toute les traces numériques afférentes et présentes sur les ordinateurs et Internet.

Légende :

✔ Convergence entre ce qui est dit dans les chartes et les pratiques des entreprises interrogées

✖ Divergence entre ce qui est dit dans les chartes et les pratiques des entreprises interrogées, identification de problèmes

Bibliographie générale

Ouvrages généraux

ACTES DU COLLOQUE, *Les Français et leurs archives*, au Conseil économique et social du 5 novembre 2001, Fayard, 2002, 227 p.

AFDA, *Les droits publics subjectifs des administrés*, Travaux de l'AFDA - 4, LexisNexis Litec, Collection Colloques et Débats, 2011, 238 p.

AMBROSE M.L, AUSLOOS J, *The Right to Be Forgotten across the Pond*, Journal of information Policy, 2013/3, 1 à 23 pp.

ARAMAZANI A, *Le droit à l'oubli et internet*, R.D.T.I., 2011/2, 34 à 49 pp.

ARENDT H, *Condition de l'homme moderne*, Calman-Lévy, Paris, 1983. On Revolution, Penguin Classics, London, 1963.

AUSLOOS J, *The 'Right to be Forgotten - Worth remembering? Computer Law & Security Review*, núm. 28, 2012, 143 à 152 p.

Benejat M, *les droits sur les données personnelles*, in *les droits de la personnalité*, sous la direction de j.-ch. Saint pau, lexis-nexis, 2013.

Benett C.J, Molnar A, Parsons C, *Forgetting, Non-forgetting and quasi-forgetting in social networking: canadian policy and corporate practice*, WWW.SSRN.COM/ABSTRACT=2208098

BENTHAM J, *Le panoptique*, belfond, 1977.

BENYEKHLEF K, *Minors, social network sites and le droit à l'oubli*, Rapport rédigé pour la Fundacion Solventia, Madrid, Espagne, Mars 2010, 40 p (avec Philippe-Antoine Couture-Ménard et Emmanuelle Paquette-Bélanger).

BERGUIG M, THIERACHE C, *L'oubli numérique est-il de droit face à une mémoire numérique illimitée ?*, Revue Lamy droit de l'immatériel, juillet 2010, n° 62, 34 à 38 pp.

BERNAL P. A, *A Right to Delete?* European Journal of Law and Technology, 2011, Vol. 2, Issue 2, 1 à 18 pp.

BOULANGER M.-H, DE TERWANGNE C, *Internet et le respect de la vie privée*, in E. MONTERO (sous la coordination de), *Internet face au droit*, Cahiers du Centre de Recherches Informatique et Droit, n° 12, 1997, Namur, C.R.I.D.-Story Scientia, 1997, 189 à 213 pp.

BRUGUIERE J.-M, GLEIZE B, *Les droits de la personnalité*, à paraître.

Cabrillac R, Frison-Roche M.A., Revet T, *Droits et libertés fondamentaux*, Dalloz, 2012.

Carbonnier J, Droit civil *Les biens, Les obligations*, PUF, 2004.

CARON C, *A propos du conflit entre les œuvres de fiction et la vie privée*, D. 2003, 1715 p.

CASTELLANO P. S, *The right to be forgotten under European Law: a Constitutionnal debate, Lex Electronica, vol. 16.1, winter 2012, 30 p.*

COHENDET M-A, *Droit constitutionnel*, Montchrestien, 3e éd., 2006, 440 p.

CONLEY CH, *The Right to Delete*, AAAI Spring Symposium Series, North America, 2010, 53 à 58 pp. (http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482).

Cornu G, *Vocabulaire juridique*, association h. capitant, puf.

CORTÉS C, *Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital* (http://www.palermo.edu/cele/pdf/DerechoalolvidoiI.EI.pdf).

DEFREYNE E, *Le droit à l'oubli numérique et les archives journalistiques*, R.D.T.I., 2013/2, 75 à 98 pp.
DE TERWANGE C, *Privacidad en Internet y el derecho a ser olvidado/derecho al olvido* , IDP Revista de Derecho, Internet y Política, núm. 13, 2012, 53 à 66 pp. *Internet Privacy ans the Right to be forgotten/right to Oblivion* , Revista d'Internet, dret i política, 2012/13, 109 à 121 pp. *Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles*, Petites affiches, 2005/194, 40 à 48 pp.
DUMORTIER F, *Facebook and risks of de-contextualization of information*, 2009, disponible à http://works.bepress.com/franck_dumortier/1
ENISA, *The right to be forgotten – between expectations and practice*, European Network and Information Security Agency, 20 de noviembre de 2012, 1 à 22 pp.
(http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten).
ETTIGHOFFER D, *Les droits de « l'Homme Numérique » : le droit à l'oubli*, www.ettighoffer.com
FAVIER J, *Les archives*, PUF, Que sais-je ?, 5e éd. recorrigée, 1991, 127 p.
FAVOREU L, ET A, *Droit constitutionnel*, Dalloz, Précis droit public science politique, 16e éd., 2014, 1070 p.
FAZLIOGLU M, *Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet*, *International Data Privacy Law*, vol. 3, núm. 3, 2013, 149 à 157 pp.
FLEISCHER P, *Foggy Thinking about the Right to Oblivion*, 9 de Marzo de 2011. (http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html).
The Right to be Forgotten, seen from Spain, 5 de septiembre de 2011.
(http://peterfleischer.blogspot.com/2011/09/right-to-be-forgotten-seen-from-spain.html)
The right to be forgotten, or how to edit your history, 29 de enero de 2012,
http://peterfleischer.blogspot.co.uk/2012/01/right-to-be-forgotten-or-how-to-edit.html).
FOUCAULT M, *Sécurite, territoire, population* : cours au college de france (1977-1978) seuil, 2004. Surveiller et punir Gallimard, 1993.
Frayssinet J, L'internet et la protection juridique des données personnelles. L'internet et le droit, éd. Victoires, 2001.
FREUD S, *Métapsychologie. Folio, 1986.*
KOOPS B.-J, *Forgetting footprints, shunning shadows. A critical analysis of the "right to be forgotten" in big data practice*, December 2011, disponible à l'adresse www.ssrn.com
LASSERRE B, LENOIR N ET STIRN B, *La transparence administrative*, PUF, Politique d'aujourd'hui, 1987, 236 p.
LEGRAND F, BELLAMY A, *Touche pas à ma e-réputation! Enquête*, 6 avril 2012.
http://www.lesnumeriques.com/divers/touche-pas-a-e-reputation-enquete-a1548.html
Lepage A, Droit à l'oubli, une jurisprudence tâtonnante, Dalloz. 2001, 2079 p.
LETTERON R, *Le droit à l'oubli*, Revue de droit public et de la science politique en France et à l'étranger, 1996/2, 385 à 424 pp.
LEVINAS E, *Totalite et infini* Springer, 1984.
LOCKE J, *Essai sur l'entendement humain*, Paris, Vrin, 2001.
Lucas-Schloetter A, Nature du droit d'auteur, Droit d'auteur et droits de la personnalité, JCl. Civil Annexes, Fasc. 1118.
Lucas A, Deveze J, Frayssinet J, *Droit de l'informatique et de l'Internet*, PUF, Paris, 2001.
malaurie p, aynes l, stoffel-munk p, *Les obligations*, 5e éd., 2011.
MALLET M.-L, *L'animal autobiographique* ga, 1999.

MALLET-POUJOL N, *Du droit à l'oubli numérique*, RD&J, 2011/37, 9 à 10 pp.
Marais A, Le droit à l'oubli numérique in B. Teyssié (dir.), La communication numérique, un droit, des droits, Ed. Panthéon-Assas, 2012, 63 s p.
MAYER-SCHÖNBERGER V, *Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing*, John F. Kennedy School of Government Faculty Research Working Paper Series, RWP07-022, April 2007, www.vmsweb.net.
MAYER-SCHÖNBERGER V, *Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing*, Harvard University, April 2007, 1 à 24 pp.
http://www.vmsweb.net/attachments/pdf/Useful_Void.pdf). *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Oxford, 2009.
Merle Ph, *Droit commercial, Sociétés commerciales*, 16e éd. Dalloz, Précis, 2013.
MOINY J.P, *Facebook au regard des règles européennes concernant la protection des données*, European Journal of Consumer Law, 2010, 235-271 pp.
MONTELS B, *Un an de droit de l'audiovisuel*, Communication Commerce électronique, n°6, 2013, chron. 6.
NIETZCHE F, *La généalogie de la morale, in Œuvres*, éd. par Jean Lacoste et Jacques Le Rider, Robert Laffont, éd. Bouquins, Paris, 1993. *Considérations inactuelles. De l'utilité et des inconvénients des études historiques,* éd. Mercure de France, Paris 1873.
NIGER S, *Il diritto all'oblio, Diritto all'anonimato: anonimato, nome e identitá personale,* G. Finocchiaro (ed.), Cedam, Padua, 2008, 59 à 73 pp.
NUNO GOMES DE ANDRADE N, *Oblivion : The Right to Be Different ... from Oneself. Reproposing the Right to Be Forgotten*, Revista d'Internet, dret i política, 2012/13, 122-137 pp.
NYS H, *Towards a Human Right 'to Be Forgotten Online'?* European Journal of Health Law, núm. 18, 2011, 469 à 475 pp.
Poncela P, *Les liaisons dangereuses du droit à l'image et du droit à l'information du public*, Chronique de l'exécution des peines, RSC juillet/septembre 2012, 649 s p.
PROUST M, *À la recherche du temps perdu.* XIII Albertine disparue, Gallimard, Paris, 1925.
RALLO A, *A partir de la protección de Datos. El derecho al olvido y su protección*, TELOS. Cuadernos de Comunicación e Innovación (Los derechos fundamentales en Internet), 2010, 104 à 108 p.
Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma, Revista de Derecho Político, núm. 85, septiembre-diciembre, 2012, 13 à 56 p. »
Data Protection, Social Networks, and Online Mass Media (with R. Martínez), European Data Protection: Coming of Age, Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet Editors, ed. Springer, London-New York, 2013, 407 à 430 p.
La protección de la privacidad en las redes sociales de Internet: la experiencia canadiense con facebook, google y otros Derecho y Redes Sociales, A. Rallo Lombarte y R. Martínez Martínez (Editores), 2ª edición, Civitas-Thomson Reuters, Pamplona, 2013, 257 à 284 p.
RANGEON F, *Information et transparence administrative*, PUF, 1988, 280 p.
ROSEN J, *Free speech, privacy and the web that never forgets*, Telecommunications and High Technology Law, vol. 9, 2011, 346 à 356 p.
The right to be forgotten, Stanford Law Review Online, vol. 64, 2012, 88 à 92 p.
ROUVROY A, *Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ?* , Avril 2008, http://works.bepress.com/antoinette_rouvroy/5, 33 p.

ROUVROY A, POULLET Y, *The right to informational self-determination and the value of self-development. Reassessing the importance of privacy in democracy*, in Reinventing Data-Protection? Springer, 2009, 45 à76 pp.
Saint-Pau J-C, *Jouissance des droits civils, Droit au respect de la vie privée, Régime, Atteinte à la vie privée*, JCl. Civil Code, Fasc. 15. (Sous la dir.), Droits de la personnalité, Lexisnexis, coll. Traités, 2013.
SARTOR G, Y VIOLA DE AZAVEDO CUNHA M, *The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, International Journal of Law and Information Technology, vol. 18-4, 2010, 356 à 378 pp.
SIMÓN CASTELLANO P, *El régimen constitucional del derecho al olvido digital,* Tirant lo Blanch, Valencia, 2012.
Slama S, Contrariété à la loi pénitentiaire d'une autorisation de diffusion télévisuelle d'un documentaire conditionnée à l'anonymat physique et patronymique des détenus in Lettre « Actualités Droits-Libertés » du credof, 14 août 2012.
SOLOVE, D.J, *The future of reputation: gossip, rumor, and privacy on the Internet*, New Haven and London, Yale University Press, 2007. *I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, San Diego Law Review, vol. 44, 2007, 745 à 772 pp.
STROWEL A, *Liberté de rappeler des faits contre droit au silence : les contretemps de la presse* », note sous Civ. Namur, 17 novembre 1997, J.L.M.B., 1998, 785 et s pp.
SZÉKELY I, *The right to forget, the right to be forgotten. Personal reflections on the fate of personal data in the information society* », in S. Gutwirth, R. Leenes, P. De Hert and Y. Poullet (eds.), *European data protection: in good health?,* Dordrecht, Springer, 2012, 347-363 pp.
TRUCHET D, *A propos du droit à l'oubli et du devoir de mémoire*, Libertés, Justice, Tolérance. Mélanges en hommage au Doyen Gérard Cohen-Jonathan, Vol. II, Bruxelles, Bruylant, 2004, 1595 à 1603 pp.
TRUDEL P, *L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes*, http://www.chairelrwilson.ca/cours/drt6913/Notes%20oubli3808.pdf). *Moteurs de recherche et respect de la vie privée: version préliminaire*, Rapport pour la Journée *« L'économie et le droit des moteurs de recherche »*, Paris, 16 de mayo de 2008. « *La menace du droit à l'oubli* », 5 oct 2013 (http://blogues.journaldemontreal.com/pierretrudel/droit/la-menace-du-droit-a-loubli/).
VAN ENIS Q, *Le temps ne fait rien à l'affaire…* Les archives du Times devant la Cour européenne des droits de l'homme, note sous Cour eur. D.H., 10 mars 2009, Times Newspapers Limited (n° 1 et 2) c. Royaume-Uni, R.D.T.I., 94 à 103 pp.
WEBER R. H, *The Right to Be Forgotten: More Than a Pandora's Box?,* Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 2, 2011, 120 à 130 pp (http://www.jipitec.eu/issues/jipitec-2-2-2011/3084).
WERRO F, *The right to Inform v. the Right to be forgotten: A transatlantic Clash,* in Liability in the Third Millenium, 285-300.
WITTGENSTEIN L, *Le Cahier bleu et le Cahier brun* (tr. fr. Goldberg et Sackur), Gallimard, Paris, 1996.

Monographies, essais, thèses

AUGE M, *Les Formes de l'oubli*, Rivages poche, Paris, 2001.

BERNS T, *Gouverner sans gouverner; une archéologie politique de la statistique*, Presses universitaires France, 2009.
BRANSCOMB A.W, *Who Owns Information?* From Privacy to Public Access, Basic Books, New York, 1994.
CONNOLLY CH, *Galexia, The US Safe Harbor – Fact or Fiction ?*, Pyrmont (Australie), 2008, publié in Privacy Laws and Business International, issue 96, 2008, p. 1, 3, 26-27.
COOKE E, *The Modern Law of Estoppel*, OUP, Oxford, 2000.
DARGENT J, *La doctrine de l'estoppel.Une théorie originale du droit anglais en matière de preuve*, Imprimerie Georges Frère, Tourcoing, 1943.
EISENSTEIN E.L, *The Printing Revolution in Early Modern Europe*, Cambridge University Press, Cambridge, 1993.
FLAHERTY D, *Privacy in Colonial New England*, University Press of Virginia, Charlottesville, 1972.
FOGEL J. F. ET PATINO B, *La condition numérique*, Grasset, 2013.
FOULQUIER N, *Les droits publics subjectifs des administrés. Émergence d'un concept en droit administratif français du XIX^e siècle au XX^e siècle*, Dalloz, Nouvelle Bibliothèque de Thèses, 2000, 805.
FRIEDMAN L.M, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*, Stanford University Press, Stanford, 2007.
GARINOT J.-M., *Le secret des affaires*, LexisNexis, 2013.
HARDOIN-LE GOFF C, *L'oubli de l'infraction*, LGDJ, Paris, 2008.
KAYSER P, *La protection de la vie privée par le droit : protection du secret de la vie privée*, 3^e éd., PUAM, Economica, Aix-en-Provence, Paris, 1995.
KESSOUS E, *L'attention au monde*, Armand collin, 2012.
LANE F.S, *American Privacy: The 400-Year History of our Most Contested Right*, Beacon Press, Boston, 2011.
MACINTYRE A, *After virtue: a study in moral theory university of notre dame*, Press, 1984.
MARTRON H, *Les droits de la personnalité des personnes morales de droit privé*, LGDJ 2011.
MASON A.TH, *Brandeis: A Free Man's Life*, The Viking press, New York, 1946.
MAURER H, *Droit administratif allemand*, (trad. M. Fromont), LGDJ, Paris, 1995.
MAYER-SCHÖNBERGER V, *Delete.The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton, Oxford, 2009.
MILTON J, *Pour la liberté de la presse sans autorisation ni censure*, Areopagitica, éd. bilingue, (trad. O. Lutaud), Aubier-Flammarion, Paris, 1969.
NOWAK R.D, ROTUNDA J.E, *Treatise on constitutional law: substance and procedure*, Thomson/West, éd. électr. Westlaw, 2013.
ORTH J.V, *Due Process of Law.- A Brief History*, University Press of Kansas, Lawrence, 2003.
PIERRE R, *Les droits fondamentaux des personnes morales de droit privé*, Limoges, 201●.
PROSSER W.L, *Handbook of the Law of Torts*, 1st ed., West Publishing Co., St. Paul, 1941.
PROSSER W.L, *Handbook of the Law of Torts*, 2nd ed., West Publishing Co., St. Paul, 1955.
PROSSER W.L, *Handbook of the Law of Torts*, 4th ed., West Publishing Co., St. Paul, 1971.
REGAN P, *Legislating Privacy : Technology, Social Values and Public Policy*, University of North Carolina Press, Chapel Hill, N.C, 1995.
RICŒUR P, *La mémoire, l'histoire, l'oubli*, Éditions du Seuil, Paris, 2000, 2007.
RIGAUX F, *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, LGDJ, Bruxelles, Paris, 1990.
RIGAUX F, *La vie privée.- Une liberté parmi les autres ?*, Larcier, Bruxelles, 1992, p. 1-20.

RUSSELL I.S, BUCHOLTZ B.K, *Mastering Contract Law*, Carolina Academic Press, Durham, 2011.
SAINT-JAMES V, *La conciliation des droits de l'homme et des libertés en droit français*, PUAM, 1995, 476 p.
SOLOVE D.J, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, London, 2011. *Understanding Privacy*, Havard University Press, Cambridge, London, 2008.
SOLOVE D.J, SCHWARTZ P.M, *Information Privacy Law*, 4th ed., Wolters Kluwer, New York, 2011.
STUART MILL J, *De la liberté* (trad. Dupont-White), Guillaumin et Cie, Libraires, Paris, 1860.
SUDRE F, *Droit européen et international des droits de l'homme*, 10e éd., PUF, Paris, 2011.
SULLIVAN E.TH, FRASE R.S, *Proportionality Principles in American Law.Controlling Excessive Government Actions*, Oxford University Press, Oxford, New York, 2009.
TAYLOR C, *Les sources du moi : la formation de l'identité moderne,* Seuil, 1998.
VAN DROOGHENBROECK S, *La proportionnalité dans la convention européenne des droits de l'homme.- Prendre l'idée simple au sérieux*, Bruylant, Publications des Facultés universitaires Saint-Louis, Bruxelles, 2001.
VIVANT M, ALI I, *Informatique, Multimédia, Réseaux, Internet*, Lamy droit du numérique. Éditions Lamy, Paris, 2012.
ZOLLER E, *Les grands arrêts de la Cour suprême des États-Unis*, 1re éd., Dalloz, Grands arrêts, Paris, 2010.

Articles

AUBY J-B, « La bataille de San Romano - Réflexions sur les évolutions récentes du droit administratif », AJDA, 2001, p. 912. « Droit administratif et démocratie », Droit administratif, 2006, n° 2, p. 6.
BAILLEUL D, « Le droit administratif en question : de l'intérêt général à l'intérêt économique général ? », JCP A, 2005, n° 13, p. 587.
Bennett C, « International Privacy Standards: can Accountability be Adequate? », Privacy Laws and Business International, 2010 - colinbennett.ca.
BONNARD R, « Les droits publics subjectifs des administrés », *RDP*, 1932, p. 695.
BOURBOULOUX H, « Le décret du 2 septembre 2013 : le droit à l'oubli tout relatif des dirigeants ayant connu une procédure collective », JCP E, n° 46, 14 Novembre 2013, act. 821.
BRAIBANT G, « Droit d'accès et droit à l'information, Mélanges R. E. Charlier, service public et libertés », éd. de l'Université, 1981, p. 703. Préface, « La transparence administrative », PUF, Politique d'aujourd'hui, 1987, p. I. « Le passé et l'avenir de l'administration publique », *RFAP*, 2002, n° 102, p. 213.
CAPRIOLI A, Loi du 6 août 2004. « Commerce à distance sur Internet et protection des données à caractère personnel », Comm. com. électr. n°2, févr. 2005.
CARTIER E, « Histoire et droit : rivalité ou complémentarité ? », RFD const. 2006, n° 67, p. 509.
Catala P, « Actualité du droit de l'Internet », CCE juin 2003, Repères, P.3.
CHABIN M-A, « La communicabilité des archives : l'information, le document, le dossier », La revue administrative, 1995, n° 283, p. 415.
CHAMINADE A, « Accès aux documents administratifs et aux archives publiques. À propos de l'ordonnance du 29 avril 2009 », *JCP A*, 2009, n° 25, actu. 739.
CHEVALLIER J, « Les fondements idéologiques du droit administratif français, Variations autour de l'idéologie de l'intérêt général », CURAPP, PUF, 1979, tome II, p. 3. « L'État-Nation », *RDP*,

1980, p. 1285. « Le mythe de la transparence administrative », Information et transparence administrative, PUF, 1998, p. 239. « La transformation de la relation administrative : mythe ou réalité ? » (à propos de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations) , Dalloz, 2000, p. 575. « De l'administration démocratique à la démocratie administrative », *RFAP*, 2001, n° 137 -138, p. 217.

CHICOT P-Y, « La démocratie représentative : essai de conceptualisation », La revue administrative, 2011, n° 380, p. 138.

CHIRAC J, Discours, « Les Français et leurs archives », actes du colloque du 5 novembre 2001, Fayard, 2002, p. 162.

cohen-tanugi l, « Le nouvel ordre numérique », In: Réseaux, 1999, volume 17 n°97. P.172

Costaz C, « Le droit à l'oubli », Gaz. Pal, 27 juillet 1995, II, doctr. P. 961.

CORNU G, « Association Henri Capitant, Vocabulaire juridique », Puf, 7ème édition

DAUGERON B, « La démocratie administrative dans la théorie du droit public : retour sur la naissance d'un concept », *RFAP*, 2011, n° 137-138, p. 21.

DE BOISDEFFRE M, « Administration et archives aujourd'hui », *RFAP*, 2002, n° 102, p. 277.

De Lamberterie I, « Informatique, Libertés et opinions religieuses, Archives des sciences sociales des religions », 1995, Volume 91, n°1, P.21- 39

DELAUNAY B, « Nouvelles limitations à l'accès aux documents administratifs », note sous CE, 17 avril 2013, n° 342372, n° 344924, n° 337194, AJDA, 2013, p. 1920.

DELEUZE G, « Post-scriptum sur les sociétés de contrôle », in Pourparler, Paris, Éditions de Minuit, 2003.

DELMAS B, « Une nouvelle loi sur les archives : « des archives plus riches et plus ouvertes ? », La revue administrative, 2008, n° 361, p. 371.

DELVOLVÉ P, « Propos introductifs. Droits publics subjectifs des administrés et subjectivisation du droit administratif », Les droits publics subjectifs des administrés, Travaux de l'AFDA - 4, LexisNexis Litec, Collection Colloques et Débats, 2011, p. 3.

DERIEUX E, « La notion de « publication - Les insupportables incertitudes du droit », *JCP G*, 2010, n° 49, 1195.

DONIER V, « Les droits de l'usager et ceux du citoyen, RFDA, 2008, p. 13. Les lois du service public : entre tradition et modernité », RFDA, 2006, p. 1219.

DOUILLARD J, « La communicabilité des archives départementales aux sociétés privées : entre orthodoxie et éthiques législatives », JCP A, 2010, n° 35, actu. 608.

DUCLERT V, « République et archive », RFAP, 2002, n° 102, p. 269.

Dumoulin L, « Les droits de la personnalité des personnes morales », Revue des sociétés, 2006, p. 1

Dupré De Boulois X, « Les droits fondamentaux des personnes morales » : 1ère partie, RDLF 2011, chron. n°15 ; 2ème partie, RDLF 2011, chron. n°17 ; 3ème partie, RDLF 2012, chron. n°01.

DURANTON M ET FOEGLE J-P, « Fichage partout, oubli nulle part ? Le Conseil d'État ouvre un boulevard au fichier "TAJ" », Revue des droits de l'homme, 16 juillet 2014.

EVEN P, « Une nouvelle loi pour les archives », La revue administrative, 2009, n° 367, p. 231.

FAVREAU A, « La délibération de la CNIL du 12 juillet 2011 : une pierre dans l'édifice du droit à l'oubli», Revue Lamy Droit civil, 2012, n° 92, p. 53.

FOUCAULT M, « Qu'est-ce qu'un auteur ? » In Dits et Ecrits, tome 2 : 1976 - 1988 Gallimard, 2001.

Fourlon A, « Toute ressemblance avec des personnages existant ou ayant existé… Est-elle constitutive d'une atteinte aux droits de la personnalité ? « Etude de la jurisprudence rendue en matière de fictions du réel, Communication Commerce électronique, mars 2007, étude 5.
Frayssinet J, « A propos du droit d'accès des personnes morales », Expertises, oct. 1984, n°66, p. 241
Girard F, « Sens et possibilités d'un « droit à l'oubli » aux Etats-Unis », (contribution à ce rapport).
GOMES DE ANDRADE R.N, « El olvido: El derecho a ser diferente… de uno mismo. Una reconsideración del derecho a ser olvidado », IDP Revista de Derecho, Internet y Política, núm. 13, 2012, 67 à 83 pp.
KEELE B.J, « Privacy by deletion: the need for a global data deletion principle », Indiana Journal of Global Legal Studies, winter, núm. 16-1, 2009, 363 à 384 pp.
GONOD P, « La réforme des archives : une occasion manquée », AJDA, 2008, p. 1597.
GOUNIN Y, LALUQUE L, « La réforme du droit d'accès aux documents administratifs », AJDA, 2000, p. 486.
Haas G, « E-réputation, regards croisés de l'avocat et du magistrat sur l'e-réputation négative », Expertises n°332, octobre 2011.
KAYSER P, « La protection de la vie privée par le droit », 2e éd. In: Revue internationale de droit comparé.Vol.43 N°1, Janvier-mars 1991. pp. 269-271.
http://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg.
« Lachasse aux hommes », Le monde 21/03/1974.
KERVICHE E, « La Constitution, le chercheur et la mémoire », *RDP*, 2009, p. 1051.
KOUBI G, « Nuances d'un droit à la communication des documents administratifs », note sous CE, 17 avril 2013, n° 3444924, n° 342372, n° 338649, 24 avril 2013, n° 338649, n° 337982, JCP A, 2013, n° 28, 2207.
LAVAISSIÈRE J, « Le pouvoir, ses archives et ses secrets », Dalloz, 1984, chron. p. 63.
LECLERC J-P, « Le rôle de la Commission d'accès aux documents administratifs », *RFAP*, 2011, n° 137-138, p. 171.
LEGENDRE P, « Une mémoire fonctionnelle », *RFAP*, 2002, n° 102, p. 223.
LEMAIRE F, « Commentaire de la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations », Gazette Palais, 24 octobre 2000, n° 298, p. 3.
LEMASURIER J, « Vers une démocratie administrative : du refus d'informer au droit d'être informé », RDP, 1980, p. 1239.
LEPAGE A, « Droit à l'oubli : sanction de la CNIL », Comm. com. électr. n°12, déc. 2011
LETTERON R, « Le droit à l'oubli », *RDP*, 1996, p. 385.
Loiseau G, « Des droits humains pour des personnes non humaines », D. 2011, p. 2558. « Des droits patrimoniaux de la personnalité en droit français », Rev. Dr. Mc Gill, juin 1997, n°142.
MAISL H, « Une nouvelle liberté publique : la liberté d'accès aux documents administratifs », Mélanges R. E. Charlier, service public et libertés, éd. de l'Université, 1981, p. 831.
MALLET-POUJOL N, « Le double langage du droit à l'information », *Dalloz*, 2002, p. 2420. « Du droit à l'oubli numérique », Litec, RD&J, n°37, nov. 2011, p. 9.
MARAIS A, « Le droit à l'oubli numérique, La communication numérique, un droit, des droits », éd. Panthéon-Assas, 2012, p. 63.
MARCHAND J, « L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique », JCP A, 2014, n° 7, 2038.

MONIOLLE C, « Indépendance et liberté d'expression des enseignants-chercheurs », AJDA, 2001, p. 226.
MONNIER S, « La réforme du droit des archives. À propos de la loi du 15 juillet 2008 », Droit administratif, 2008, n° 11, p. 21.
NISSENBAUM H, « Protecting Privacy in an Information Age: The Problem of Privacy in Public Law and Philosophy », Springer, 1998, 17, 559-596
PETIT F, « La mémoire en droit privé », *RRJ*, 1997, n° 1, p. 17. « Les droits de la personnalité confrontés aux particularismes des personnes morales », D. Aff. 1998, N°117, p. 826
PIERRE R, « La protection européenne du droit à la réputation : de la nécessaire distinction entre personne physique et personne morale », CCE n° 5, Mai 2012, étude 10.
PONTHOREAU M-C, « La directive 95/46 CE 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 », *RFDA*, 1997, p. 125.
PUYBASSET M, « Le droit à l'information administrative », AJDA, 2003, p. 1307.
RANGEAON F, « L'accès à l'information administrative, Information et transparence administrative », PUF, 1998, p. 79.
RÉMOND R, *« Introduction, Les Français et leurs* archives », Actes du colloque du 5 novembre 2001, Fayard, 2002, p. 24.
ROBINEAU-ISRAËL A ET LASSERRE B, « Administration électronique et accès à l'information administrative », AJDA, 2003, p. 1325.
Roussel Galle P, « Droit à l'oubli…du moins au RCS…» Revue des sociétés, 2012, p. 188.
ROUVEROY A, « Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation? », Politique des algorithmes. Les métriques du web. Reseaux, Vol.31, n.177, pp. 163-196, 2013.
Trefigny P, Chronique Droit du numérique septembre 2012 - septembre 2013, Outil d'aide à la recherche et responsabilité du moteur de recherche : e-reputation sous la direction de Trefigny P Et Larrieu J D. 2013, p.2487.
THIERACHE C, « Le droit à l'oubli numérique : un essai qui reste à transformer », RLDI 2011, 67.
TRUCHET D, « À propos du droit à l'oubli et du devoir de mémoire », Mélanges en l'honneur du Doyen Gérard Cohen Jonathan, libertés, justice, tolérance, Bruylant, 2004, vol. II, p. 1595.
SALES E, « Vers l'émergence d'un droit administratif des libertés fondamentales ? », RDP, 2004, p. 207.
SEILLER B, « Avant propos, Les droits publics subjectifs des administrés » Travaux de l'AFDA - 4, LexisNexis Litec, Collection Colloques et Débats, 2011, p. 1.
SÉNAC C-E, « Le droit à l'oubli en droit public », RDP, 2012, p. 1156.
SINNASSAMY C, « L'effectivité de la transparence administrative : quelle réussite juridique ? », RRJ, 2007, n° 3, p. 1375.
SZYMCZAK D, « Le droit européen, source de droits publics subjectifs des administrés ? Les droits publics subjectifs des administrés », Travaux de l'AFDA - 4, LexisNexis Litec, Collection Colloques et Débats, 2011, p. 51.
VALLOR S, «Social Networking Technology and the Virtues Ethics and Information Technology 2010 », 12, 157-170.
VINCENT J-Y, « Accès aux documents administratifs. Régime général. Loi du 17 juillet 1978 », JurisClasseur administratif, Fasc. 109-10, 2010.

Wester-Ouisse V, « Dérives anthropomorphiques de la personnalité morale : ascendances et influences », JCP G 2009. I. 137 et « La jurisprudence et les personnes morales. Du propre de l'homme aux droits de l'homme », JCP G 2009, I, 121.

Rapports et avis

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, « Un approche globale de la protection des données à caractère personnel dans l'Union européenne », COM(2010)609, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0609:FR:NOT.

Contrôleur européen à la protection des données, avis du 14 janvier 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée - *Une approche globale de la protection des données à caractère personnel dans l'Union européenne,* J.O. C 181/01, 22 juin 2011, pp. 1 et s.

Cyberlex (L'association du Droit et des Nouvelles Technologies), Contribution dans le cadre des travaux sur le droit à l'oubli numérique. *L'oubli numérique est-il de droit face à une mémoire numérique illimitée ?,* Rapport Cyberlex – Groupe de travail DAO, 25 mai 2010, 354 p.

DÉTRAIGNE Y, ESCOFFIER A-M, « La vie privée à l'heure des mémoires numériques » (Rapport d'information, Commission des lois du Sénat), 27 mai 2009, www.senat.fr

ENISA, « The right to be forgotten - between expectations and practice », 20 November 2012, available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/

Groupe de travail « Article 29 » sur la protection des données, « Avis 01/2012 du 23 mars 2012 sur les propositions de réforme de la protection des données », www.ec.europa.eu/justice/data-protection/index_en.htm.

Commission informatique et libertés, Rapport Tricot, La Documentation française, 1975, tome 1, p. 19.
CNIL, 21ème Rapport d'activité 2000, p. 187

Rapport 2012, Le défenseur des droits : Enfants et écrans grandir dans le monde numérique.
Commission des lois du Sénat, Rapport d'information n°441 (2008-2009), La vie privée à l'heure des mémoires numériques, de Detraigne Y Et Escoffier A-M p. 35

Commission européenne, Proposition de Règlement européen et du Conseil, 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, 25 janvier 2012, COM/2012, 11 final.

Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n°108, Strasbourg le 16 octobre 2012, Propositions de modernisation adoptées par la 29e réunion plénière, T-PD(2012)4Rev4
Conseil de l'Europe, Convention STE n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ratifié par la France le 24 mars 1983 et entré en vigueur le 1er octobre 1985.

Rapport d'Henri Marte, Rapport du Groupe « Intelligence économique et stratégie des entreprises », La documentation française, 1994.

Report 22 november 2013, Committee on Civil Liberties, Justice and Home Affairs by Jan Philipp Albrecht on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free

movement of such data (General Data Protection Regulation) COM (2012)0011 – C7-0025/2012 – 2012/0011(COD).

BRAIBANT G, « Les archives en France, La documentation française », Collection des rapports officiels, 1996, 303 p.

31e Conférence internationale des commissaires à la protection des données et de la vie privée, Résolution sur des normes internationales sur la vie privée, Madrid, 4,5 et 6 nov. 2009

32e Conférence mondiale des commissaires à la protection des données et de la vie privée, Projet de 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, Jérusalem, 27-29 oct. 2010.

CNIL, 30e rapport d'activités, La Documentation française, Paris, 2009.

CNIL, 33e rapport d'activité, La Documentation française, Paris, 2012.

CNIL, Dix ans d'informatique et libertés, Economica, Paris, 1988.

CNIL, Peyrat M, La publicité ciblée en ligne, Paris, 5 févr. 2009.

Commission Staff Working Paper, Impacct Assessment, SEC (2012) 72 final, Brussels, 25.1.2012

CyberLex, Contribution dans le cadre des travaux sur le droit à l'oubli numérique, « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? », Paris, 2012.

ECIPE, The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce, ECIPE, Brussels, 2013 .

European Network and Information Security Agency (enisa), the right to be forgotten – between expectations and practice, Heraklion, 2011.

FTC, Office of the General Counsel, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, FTC (July 2008) .

FTC, Privacy Online : Fair Information Practices in the Electronic Markeplace.- A Report to Congress, FTC, May 2000.

FTC, Protecting Consumer Privacy in Era of Rapid Change: Recommendations for Businesses and PolicyMakers, 2012.

G29, Avis 01/2012 sur les propositions de réforme de la protection des données, 00530/12/FR, WP 191, 23.03.2012, p. 15

G29, Avis 4/2007 sur le concept de données à caractère personnel, 01248/07/FR, WR 136, 20.06.2007.

G29, Avis 5/29 sur les réseaux sociaux en ligne, 12 juin 2009, 01189/09/FR, WP 163

G29, Avis n° 3/2010 sur le principe de la responsabilité, 13 juill. 2010, 00062/10/FR WP 173

G29, Letter adressed to Google by the Article 29 Group Brussels, 16.10.2012

G29, Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN WP 192, 22 March 2012.

LA RUE F, « Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression». - Summary of cases transmitted to Governments and replies received, United Nations, General Assembly, 27 May 2011, A/HCR/17/27/Add.1

« Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens», July, 1973

Report to the Chief Judge of the State of New York, February, 2004

Sénat, Informatique et Libertés, Discussion d'un projet de loi, Sénat, Séance du 17 nov. 1977, JORF année 1977-1978, n° 77 S.

THYRAUD J, Rapport n° 72 (1977-1978) fait au nom de la commission des lois, relatif à *l'informatique* et aux *libertés*, déposé le 10 novembre 1977
UK Ministry of Justice, Impact Assessment on Proposal for EU Data Protection Regulation, 22.11.2012
White House, Consumer Data Privacy in a Networked World : A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, February 2012, Washington (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf)
White House, The Framework for Global Electronic Commerce, 1997
http://clinton4.nara.gov/WH/New/Commerce/

comm. 115 sous CNIL, délib. n° 2011-238 de la formation restreinte, 12 juill. 2011 : www.cnil.fr
comm. 54 sous TGI Paris, réf. 15 févr. 2012
TGI Paris, 14 janv. 2013, 17ème ch., RG n° 11/03875
CNIL, formation restreinte, délib. n°2011-238, 12 juill. 2011, www.cnil.fr
TGI Paris, 14 janv. 2013, 17ème ch., RG n° 11/03875
loi n° 78-17 du 6 janvier 1978, art. 38, modifié par la loi n°2004-801 du 6 août 2004

Chartes

Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche, du 13 oct. 2010
Charte sur la publicité ciblée et la protection des internautes, du 30 sept. 2010

Notes de jurisprudence

TGI Paris, 14 avril 2008, n°08/52010, note J. Lacker, Google sage comme une image ? Ou l'application du droit américain à un site à destination du public français : RLDJ oct. 2008, n°42, P.19

Jurisprudence

TGI Paris, référé, 19 octobre 2006, Mme H.P. c/ Google France
TGI Paris, 14 avril 2008, ordonnance des référés, Madame X c/ Google
TGI de Montpellier 28 octobre 2010, ordonnance des référés, Mme C. / Google France et Inc.
TGI de Paris du 15 février 2012 Diana Z. / Google
TGI Paris 17ème chambre, 6 novembre 2013 Max M. /Google France, Google Inc
Cour de Cassation, Chambre criminelle, Affaire Sofres, 12 Mai 1998, n° 96-85.900
Cour de Cassation, Chambre criminelle, 14 mars 2006, n° 05-83423, Fabrice H. / Ministère public
Cour de Cassation, Chambre criminelle, 14 décembre 2010, n° 10-80.088
Conseil d'Etat, 9 Juillet 1997, Affaire Syntec
CJCE, 25 juillet 1991, affaire Factortame C-221/89

Textes nationaux et européens

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

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

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
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676
Directive 95/46 du Parlement 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.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:FR:PDF
Proposition de règlement du parlement européen et du conseil du 25 janvier 2012 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 (règlement général sur la protection des données)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF

Projet de rapport du 16 janvier 2013 sur la proposition de règlement du parlement européen et du conseil du 25 janvier 2012 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 (règlement général sur la protection des données)
http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-501.927&format=PDF&language=FR&secondRef=04

Rapport sur la proposition de règlement du parlement européen et du conseil du 25 janvier 2012 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 (règlement général sur la protection des données), tel que voté en commission (LIBE) le 21 novembre 2013 (version anglaise seule disponible).
CA Paris, 4ème ch, 30 avril 2003, RG 2001/14371.
CA Paris 24 septembre 2008, Vente.privée.com c/ Kalypso.
Crim., 12 oct. 1976, no 75-90.239 , Bull. crim., no 287.
Crim. 7 novembre 1936, Gaz. Pal. 1936, 2, 944.
Civ. 2ème 28 janvier 1954, in Capitant H, Terre F, Lequette Y, « Les grands arrêts de la jurisprudence civile », Dalloz, 12e éd., Tome 1
Cass. ass. Plén., 12 juill. 2000, D. 2000. Somm. 463, obs. Jourdain ; RTD civ. 2000. 842, obs. Jourdain ; ibid. 845, obs. Jourdain ; Légipresse, oct. 2000, n° 75, concl. M. le Premier avocat général Joinet.
Com., 15 mai 2012, D. 2012. 2285, obs. X. Delpech, note B. Dondero ; D. 2012. 2688, obs. J.-C.

Hallouin E, lamazerolles et rabreau a., Revue des sociétés 2012. 620, note P. Stoffel-Munck, RTD civ. 2013. 85, obs. Hauser J., JCP E 2012. 1510, note R. Mortier.
Civ. 1re, 19 juin 2013, n° 12-17.591, Lyonnaise de garantie c/ Google Inc., Google France et M. X, D. 2013, p.2487 obs. trefigny p., CCE 2013. Comm. 94 ; JCP 2013. 907, note lepage a.
CEDH 6 avril 2000, n°35382/97, Sté Comingersoll
CEDH, 15 févr. 2005, n° 68416/01, Steel et Morris c/ Royaume-Uni
CEDH, 27 mars 2008, n° 26698/05, Tourkiki Enosi Xanthis et a. c/ Grèce
CEDH, 19 juill. 2011, n° 23954/10, Uj c/ Hongrie

Connil D, note « Réutilisation commerciale d'archives départementales : nouvelle décision, nouvelle étape », sous CAA Lyon, 4 juillet 2012, n° 11LY02325, AJDA, 2013, p. 301.
Diana Z, Google, www.legalis.net.

TABLE DES MATIERES