Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ?

De Terwangne, Cécile

Published in:
Le droit à l'oubli numérique

Publication date:
2015

Document Version
le PDF de l'éditeur

CHAPITRE 1

DROIT À L'OUBLI NUMÉRIQUE, ÉLÉMENT DU DROIT À L'AUTODÉTERMINATION INFORMATIONNELLE ?

Cécile DE TERWANGNE
Professeur à la Faculté de Namur, Centre de recherche, Information, Droit et Société (CRIDS), Belgique

Introduction*

1 Le droit à l'oubli est aujourd'hui au cœur 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 œuvrant 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(1). 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 numérique.

* La rédaction de la présente contribution a été achevée en janvier 2014.
(1) Voy. *infra*, Sect. 4, §§ 1 et 2.

SECTION 1

Définition et contexte du droit à l'oubli

§ 1 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[2]. L'idée est de veiller à ce que 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 »[3]. Le droit à l'oubli, en ce sens, est lié à la finalité du traitement des données et à l'expiration

(2) 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 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 », http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF).

(3) Comm. 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, « The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age », *op. cit.*

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[4] publiée en janvier 2012 par la Commission européenne dans le but de remplacer la directive 95/46[5] accentue davantage le rôle déterminant de la volonté de l'individu en ce qui concerne le droit à l'oubli.

Cette évolution reconnaît le droit à l'oubli comme un élément de l'autodétermination informationnelle (voy. les développements au pt 2, *infra*). 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. 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.

§ 2 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[6]. Or, la mémoire peut être celle de la rancune, de la vengeance et du dénigrement[7]. Grâce à son *eternity effect*[8], 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

(4) C.E., Prop. de Règl. 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.

(5) Dir. 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, *JOCE*, L 281 du 23 novembre 1995, pp. 31-50.

(6) I. Szekely, « 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 et Y. Poullet (eds), *European data protection: in good health?*, Dordrecht, Springer, 2012, pp. 347-363.

(7) D. Ettighoffer, « Les droits de l'homme numérique : le droit à l'oubli », disponible sur www.ettighoffer.com/fr/idees/idees8.html

(8) S. Walz, « 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.

ou malhonnêtes deviennent très faciles sur le Net. Ils pourront être utilisés par quiconque veut mettre son prochain en difficulté »[9]. La Commissaire européenne à la justice Viviane Reding s'est exclamée il y a quelque 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 »[10].

La dé-contextualisation

4 Le « nouveau » droit à l'oubli numérique 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 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[11].

On a en conséquence vu apparaître des entreprises spécialisées dans la gestion de la « e-réputation » des individus et des entités juridiques sur Internet.

(9) D. Ettighoffer, « Les droits de l'homme numérique : le droit à l'oubli », *op. cit.*

(10) 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, 30 novembre 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700.

(11) Sur le risque de dé-contextualisation dans les réseaux sociaux, voy. F. Dumortier, « Facebook and risks of "de-contextualization" of information », 2009, disponible sur 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).

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 »[12]. 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[13]. L'exercice du droit à l'oubli va dès lors à l'encontre du courant économique naturel[14].

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) Notre traduction : « Nowadays forgetting is a costly affair » (I. Szekely, « The right to forget, the right to be forgotten. Personal reflections on the fate of personal data in the information society », *op. cit.*)

(13) *Ibid.*

(14) 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 », *JOUE*, C 181/01 du 22 juin 2011.

SECTION 2

Le droit à l'autonomie informationnelle ou à l'auto-détermination informationnelle

§ 1 La notion d'autonomie/auto-détermination informationnelle

7 Le droit à l'autonomie ou à l'autodétermination 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[15]. 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[16], 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

(15) C. de Terwangne, « Internet Privacy and the Right to Be Forgotten/Right to Oblivion », *Revista de Internet, Derecho y Política*, 2012, p. 112, disponible sur www.idp.uoc.edu ; A. Rouvroy et 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 K. Benyekhlef et P. Trudel (éds), *État de droit et virtualité*, Montréal, Thémis, 2009, pp. 157-222, disponible 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, pp. 8-16 ; C. de Terwangne, « Le rapport de la vie privée à l'information », in E. Montero (dir.), *Droit des technologies de l'information. Regards prospectifs*, Cahiers du CRID n° 16 Bruxelles, Bruylant, 1999, p. 144 ; Th. Léonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in F. Rigaux (dir.), *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 et C Schnabel, « Data protection in Germany I: The population census decision and the right to informational self-determination », *Computer Law & Security Rev.*, 2009, pp. 84-88 ; P. Schwartz, « The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination », *Am. J. Comp. L.*, vol. 37, n° 4, 1989, pp. 675-701, disponible sur scholarship.law.berkeley.edu/facpubs/866.

(16) 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, de la Convention européenne des droits de l'homme, voy. Cour eur. D.H., arrêt du 7 mars 2006, *Evans c. Royaume-Uni*, req. n° 6339/05 (confirmé par gde ch. dans son arrêt du 10 avril 2007) ; arrêt du 20 mars 2007, *Tysiac c. Pologne*, req. n° 5410/03 ; arrêt du 1er juillet 2008, *Daroczy c. Hongrie*, req. n° 44378/05.

première fois par la Cour constitutionnelle allemande dans sa décision cruciale de 1983[17].

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 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*[18].

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 (Conv. EDH).[19] La Convention 108 du Conseil de l'Europe[20] 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[21] 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 « [t]oute 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[22] 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'autodétermination informationnelle n'est pas absolu. Des intérêts publics ou privés prépondérants doivent être pris en

(17) BundesVerfassungsGericht, 15 décembre 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 ».

(18) Résol. 1165(1998) de l'Ass. parl. du Conseil de l'Europe sur le droit au respect de la vie privée, adoptée le 26 juin 1998 (nous soulignons).

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

(20) Conv. 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.

(21) Chartre des droits fondamentaux de l'Union européenne, *JOCE*, C-364/1 du 18 décembre 2000. Cette Charte est devenue juridiquement contraignante depuis l'entrée en vigueur du Traité de Lisbonne.

(22) Dir. 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, *JOCE*, L 281 du 23 novembre 1995, pp. 31 et s.

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[23]. Ainsi que mentionné antérieurement, les moteurs de recherche comme Google rassemblent des informations provenant de contextes variés. En œuvrant 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 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[24]. Il couvre donc les données professionnelles, les données commerciales et les données publiques.

§ 2 Le droit à l'oubli lié à l'autonomie informationnelle

9 Ainsi que déjà évoqué[25], 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

(23) « 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 sur www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/.

(24) 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) ».

(25) *Supra*, Sect. 1.

sa proposition de règlement général pour la protection des données[26], la Commission s'attaque à ces problèmes en garantissant notamment un droit à l'oubli digital (art. 17, Prop. de Règl.[27]).

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 décontextualisation, par exemple, il est vrai que les éléments remontés à la surface par les moteurs de recherche 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.

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 (Sect. 3, *infra*),
- quand le traitement des données repose sur un autre fondement que le consentement (Sect. 4, *infra*).

(26) C.E., Prop. de Règl. 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.

(27) Cette disposition est reprise dans la présente analyse en tenant également compte des modifications adoptées par le 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.

SECTION 3

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

§ 1 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 : Wikipédia, 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 disparaît 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[28]. La Commission européenne elle-même a affirmé qu'elle « avait ainsi reçu plusieurs plaintes de personnes qui n'avaient pu récupérer des données à caractère personnel

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

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 »[29].

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 reconnaître 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[30]. 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 (art. 17, § 1er) ou d'utilisation restreinte de celles-ci (art. 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 sont 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 »[31].

(29) Comm. 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.

(30) 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 ».

(31) « 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.

§ 2 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 (art. 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 envisagé dans le projet de règlement[32]. 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, p. ex., 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.

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

B. *INFORMATION DES TIERS*

15 « Afin de renforcer le droit à l'oubli numérique dans l'environnement en ligne »[33], l'article 17, § 2[34], de la proposition de règlement étend le droit à l'effacement « de façon à ce que 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 »[35].

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

(33) Considé. 54 de la Prop. de Règl.

(34) L'article 17, § 2, de la Proposition de Règlement 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 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 ».

(35) Considé. 54 de la Prop. de Règl.

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 faire effacer les données, y compris par les tiers[36]. 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[37].

Il convient de relever que la praticabilité du devoir d'information est déjà fortement contestée[38]. 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[39]. 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)[40].

(36) « [The controller] shall take all reasonable steps to have the data erased, including by third parties », 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, art. 17, § 2.
(37) « The controller shall inform the data subject, where possible, of the action taken by the relevant third parties », *ibid*. Voy. égal. « 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, amend. 121.
(38) Voy. not. l'opinion du Contrôleur européen à la protection des données, *op. cit.*, §§ 146-147.
(39) Voy. ENISA, « The right to be forgotten – between expectations and practice », 20 novembre 2012, disponible sur www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/.
(40) 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, amend. 35 et 147.

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[41]. 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 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[42]. 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.[43]. Et l'on doit aussi impérativement tenir compte de l'obligation légale de conserver certaines données à des fins de sécurité publique.

(41) 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.
(42) Voy. Sect. 4, § 2, C.
(43) C. de Terwangne et 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 sur www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_fr.pdf.

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.

§ 1 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 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.

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

- en fonction de la nature des faits en cause
- 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[44] 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 FBI 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 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[45].

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

(45) « 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.

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 »[46].

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[47]. 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.

§ 2 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 numérique nouvellement revendiqué n'était peut-être seulement que la traduction « lyrique » du droit d'opposition déjà existant[48].

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 reconnaître 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[49].

(46) 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).
(47) 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 », *LPA*, 2005, n° 194, pp. 40-48.
(48) 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, www.cyberlex.org/images/stories/pdf/contribution_cyberlex_dao.pdf.
(49) Art. 14, § 1, b), de la Dir. 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 la 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[50]. 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 raisons 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 connaître 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[51].

(50) 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... ».
(51) Sur ces critères, voy. Cour eur. D.H., 7 mars 2007, *Osterreichischer Rundfunk*.

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

À 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[52], 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 États 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* »[53].

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 § 3 ci-dessus. Les effets de l'exercice du droit à l'oubli). Ici, par exemple, le résultat pourrait être l'obligation d'effacer les données

(52) 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.

(53) Cour eur. D.H., 10 mars 2009, *Times Newspapers Limited (Nos. 1 and 2) v. the United Kingdom*, req. n° 3002/03 et n° 23676/03, § 45 (nous soulignons).

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.

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 »[54]. 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.

(54) Art. 6, § 1, e), de la Dir. 95/46.

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. À 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. égal. les remarques conclusives de la présente contribution).

§ 3 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[55]) ou l'obligation de les verrouiller. Le terme « verrouiller » a été pointé comme étant équivoque par les auteurs de la proposition de règlement[56] 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 ». À part donc la conservation des données, aucune opération ne peut plus être réalisée sur ces données, sauf dans des circonstances très limitées.

(55) 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.

(56) « Exposé des motifs », Prop. de Règl., p. 10 : « [L'article 17] intègre aussi le droit de limiter le traitement dans certains cas, en évitant le terme équivoque de "verrouillage" ».

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 ».

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[57].

(57) Voy. *supra*, Sect. 3, § 2.

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 à la section 1, paragraphe 2, 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[58]. 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 »[59]. 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* »[60].

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

(59) Conseil de l'Europe, vice-secrétaire général, « Speaking Points for the Opening the 21st T-Pd Bureau Meeting », Strasbourg, 15 novembre 2010, www.coe.int/t/dghl/standardsetting/dataprotection/151110%20DSG%20speaking%20notes%20data%20protection%20meeting%20T-PD.pdf (nous soulignons).

(60) V. Reding, « Why the EU needs new personal data protection rules? », *The European Data Protection and Privacy Conference*, Bruxelles, 30 novembre 2010, europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700 (nous 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 États 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[61].

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. À titre d'illustration d'un système de ce type, le logiciel X-Pire a été lancé en Allemagne[62]. 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.

(61) Cour eur. D.H., 4 mai 2000, *Rotaru c. Roumanie*, req. n° 28341/95. Voy. aussi l'opinion concordante du juge Wildhaber à laquelle se sont ralliés les juges Makarczyk, Türmen, Costa, Tulkens, Casadevall et Weber.

(62) www.x-pire.de/index.php?id=6&L=2.

Conclusion

30 Le droit à l'oubli numérique 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 ;
- 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 numérique 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[63], 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[64]. 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

(63) Art. 17 de la Prop. de Règl., précité.
(64) Parlement européen, Compromise amendements, précité.

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 réglementation 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 réglementation. Il perdrait assurément la visibilité que la Commission tente de lui donner et son usage par les individus 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[65]) 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, p. ex.). 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,

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

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 avais. Il a plus de chance de connaître 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.