

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Droit à l'oubli, droit à l'effacement ?

De Terwangne, Cécile

Published in:

Enjeux européens et mondiaux de la protection des données personnelles

Publication date:

2015

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

De Terwangne, C 2015, Droit à l'oubli, droit à l'effacement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique. dans *Enjeux européens et mondiaux de la protection des données personnelles*. Création information communication, Larquier , Bruxelles, pp. 245-275.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

CHAPITRE 3

DROIT À L'OUBLI, DROIT À L'EFFACEMENT OU DROIT AU DÉRÉFÉRENCEMENT ? QUAND LE LÉGISLATEUR ET LE JUGE EUROPÉENS DESSINENT LES CONTOURS DU DROIT À L'OUBLI NUMÉRIQUE

Cécile DE TERWANGNE

*Professeur à l'Université de Namur, Faculté de droit
Directrice de recherche au Centre de Recherche Information,
Droit et Société (CRIDS)*

I

Droit à l'oubli, droit à l'effacement, droit au déréférencement, de quoi s'agit-il ?

Les organisateurs du colloque sur les « Enjeux européens et mondiaux de la protection des données personnelles », dont le présent ouvrage reproduit les actes, avaient, au printemps 2014, identifié parmi ces enjeux la question de l'apport du droit à l'oubli contenu dans la proposition de règlement européen⁽¹⁾, devenu par la suite le droit à l'effacement dans le texte intermédiaire voté par le Parlement européen⁽²⁾. La décision prononcée par la Cour de justice de l'Union européenne le 13 mai 2014 dans l'affaire *Google Spain*⁽³⁾ est venue mettre remarquablement

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

(2) 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)), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf. 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.

(3) C.J.U.E., 13 mai 2014, *Google Spain S.L. et Google Inc. c. Agencia Española de Protección de Datos (AEPD)* et *Mario Costeja González*, C-131/12. Voy., parmi les très nombreux commentaires de cette décision majeure, E. DEFREYNE et R. ROBERT, « L'arrêt "Google Spain" : une clarification de la responsabilité des moteurs de recherche... aux conséquences encore floues », *R.D.T.I.*, 2015, pp. 73-114 et les références citées.

en lumière cette problématique du droit à l'oubli, sans attendre l'aboutissement des débats entre colégislateurs européens concernant le règlement en devenir.

Il est particulièrement intéressant de faire aujourd'hui l'analyse de l'article 17 de la proposition de règlement, portant sur le droit à l'oubli et/ou à l'effacement, selon les versions de la Commission ou du Parlement européens, à la lumière de ce que la Cour a déduit du texte actuel de la directive 95/46 dans l'affaire *Google Spain* concernant ce qui peut être apparenté à un élément du droit à l'oubli : le droit au déréférencement des résultats des moteurs de recherche⁽⁴⁾.

Droit à l'oubli, droit à l'effacement ou droit au déréférencement, 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 ou lorsqu'il n'est plus justifié de les maintenir dans un système d'information.

Cela avait déjà été reconnu comme un droit, dans une certaine mesure, sous deux angles différents : initialement, dans certains pays, à l'égard du passé judiciaire et ensuite, de manière limitée, en tant qu'élément du régime de protection des données à caractère personnel.

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.

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⁽⁵⁾. 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 radical 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.

Cela étant, une nuance est apportée aujourd'hui à cette notion. L'expression « droit à l'oubli » est utilisée, à tout le moins dans le cadre des institutions de l'Union européenne, pour couvrir une réalité plus vaste que le seul 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 »⁽⁶⁾. 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. En outre, la volonté de la personne concernée par les données peut également être le facteur déclencheur de ce droit à l'oubli aux contours élargis et qui n'est plus dépendant uniquement du temps écoulé.

La proposition de règlement général de protection des données publiée en janvier 2012 par la Commission européenne dans le but de remplacer la directive 95/46⁽⁷⁾ 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 III *infra*). Dans ce sens, il s'agit 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. Dans certains cas, ce droit ne devrait pas impliquer d'« arrêter de savoir », mais plutôt d'arrêter de diffuser les données ou d'arrêter de les indexer sur le 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 à un « droit au repentir ».

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 décontextualisation des données et un droit au repentir et à changer d'avis constituent le droit à l'oubli tel que nouvellement dessiné.

(4) Le « droit au déréférencement » est également appelé « droit de désindexation ».

(5) 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'Union européenne, 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*, consultable sur <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF>.)

(6) 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, « [s]i 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.).

(7) 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., L 281, 23 novembre 1995, pp. 31 à 50.

II

Contexte du droit à l'oubli numérique : les spécificités d'Internet

Les spécificités d'Internet expliquent le regain d'intérêt à l'égard d'une notion qui était jusque-là cantonnée au champ de l'évocation par les médias du passé judiciaire d'un individu. Le mode de fonctionnement d'Internet, l'effrayante caisse de résonance universelle qu'il offre aux propos et images diffusés, la capacité d'expression publique qui est désormais offerte non seulement aux médias traditionnels, mais également à tout un chacun, ont amené à revisiter le droit à l'oubli pour le transposer dans le contexte numérique découlant d'Internet.

Pour saisir les enjeux du droit à l'oubli devenu numérique, il importe de mettre en avant les spécificités d'Internet. C'est ce qui sera fait dans les paragraphes qui suivent.

A. La nécessité d'une décision d'effacer et l'« eternity effect » ou effet d'éternité qui en découle

Une des spécificités d'Internet est que, contrairement à ce qui se passe dans la vie « physique » où l'on doit déployer des efforts pour se souvenir de quelque chose et où l'oubli progressif est naturel, effacer dans le monde digital ne se réalise pas tout seul et nécessite de prendre une décision en ce sens. C'est un processus conscient et désiré. Il faut avoir la volonté de supprimer l'information.

L'infailibilité de la « mémoire totale » d'Internet contraste donc avec les limites de la mémoire humaine⁽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.

(8) 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 et Y. POULLET (éd.), *European Data Protection: in Good Health?*, Dordrecht, Springer, 2012, pp. 347 à 363.

(9) S. WALZ, « Relationship between the freedom of the press and the right to informational privacy in the emerging information society », 19^e Conférence internationale des commissaires à la protection des données, Bruxelles, 17-19 septembre 1997, p. 3.

B. Le coût économique de l'effacement

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 »⁽¹⁰⁾. 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⁽¹¹⁾. L'exercice du droit à l'oubli va dès lors à l'encontre du courant économique naturel⁽¹²⁾.

Par ailleurs, l'effacement des données à caractère personnel va à l'encontre du modèle économique d'Internet. Les cibles du droit à l'oubli sont des données, des informations pouvant être reliées à des individus. Or celles-ci sont le carburant de base du modèle économique d'Internet. 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. Leur conservation longue durée est précieuse pour les acteurs d'Internet 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, toutes deux nourries des données citées ci-dessus. Cela limite assurément l'enthousiasme à effacer de telles informations.

C. La décontextualisation des informations

Une autre caractéristique d'Internet est liée au mode de fonctionnement d'un de ses acteurs incontournables : le moteur de recherche. C'est 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, qui suscite une grande partie des préoccupations liées à l'aspiration à l'oubli. Cela débouche, en

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

(11) *Ibid.*

(12) 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.

effet, sur un portrait, composé d'éléments décontextualisés⁽¹³⁾, des individus visés par une requête à partir d'un moteur de recherche. Lié à l'« effet d'éternité » de la mémoire électronique, 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.

C'est précisément ce qui est à la base de l'affaire *Google Spain* dans laquelle un citoyen espagnol déplorait que les requêtes effectuées à partir de son nom sur le célèbre moteur de recherche débouchaient sur une liste de résultats dans laquelle figurait un article de journal mentionnant une dette fiscale qu'il avait eue par le passé mais qu'il avait apurée depuis lors.

Lorsque l'on considère les statistiques publiées par Google à propos du nombre de demandes de déréférencement que cette entreprise a reçues depuis la mise en place, à l'issue de l'arrêt de la Cour de justice du 13 mai 2014, d'un service dédié au traitement de telles demandes, on se rend compte à quel point la capacité des moteurs de recherche de faire indéfiniment remonter à la surface certaines données du passé peut conduire à des désagréments, des dommages et des souffrances pour les personnes concernées⁽¹⁴⁾.

Et ce n'est pas seulement l'information diffusée par des tiers qui peut susciter des préoccupations. L'embarras et les soucis peuvent découler de ce que l'on a mis soi-même sous les projecteurs du Web. Ce que l'on a accepté de partager avec certains destinataires parce qu'ils appartiennent à un cercle déterminé (amis, famille, membres d'un groupe d'intérêt, etc.), on ne veut 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⁽¹⁵⁾.

(13) P. TRUDEL, « L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes », *op. cit.*, pp. 2 et 3 : « Ce qui est jugé fautif et sanctionné est la redivulgateur considérée injustifiable dans le contexte où elle se produit. À ce titre, la légitimité juridique de la prétention à l'oubli se structure par l'appréciation du contexte de la diffusion de l'information. L'oubli est donc un droit pour la personne concernée lorsqu'il est jugé déraisonnable de diffuser l'information. Alors, la diffusion est jugée fautive [...]. Le contexte dans lequel s'effectue la diffusion est un facteur très important dans ce processus de détermination de son caractère fautif ».

(14) Entre juin 2014 et janvier 2015, Google a indiqué avoir reçu plus de deux cent mille demandes de déréférencement émanant des pays européens, concernant quelque huit cent mille URL (cf. sa page dédiée à la « Transparence des informations », voy. le rapport sur les « Demandes de suppression de contenus liés à la vie privée dans les résultats de recherche dans l'Union européenne », disponible à l'adresse <http://www.google.com/transparencyreport/removals/europeprivacy/?hl=fr>). Le taux de réponses positives à ces demandes, et, donc, de suppressions d'URL, a été de 40,6 %. Il est à souligner que ce nombre de demandes liées à la mise en œuvre du « droit à l'oubli » est dérisoire au regard des demandes de suppression de contenus portant atteinte au droit d'auteur, soit des demandes visant entre 6 et 8 millions d'URL... par semaine.

(15) Sur le risque de décontextualisation 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.-Ph. MOIR, « Cloud based social network sites: under whose control? », *Investigating Cyber Law and Cyber Ethics*, 2012, pp. 147 à 219).

On a, en conséquence, vu apparaître des entreprises spécialisées dans la gestion de l'« 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.

III L'autodétermination informationnelle à la base du droit à l'oubli ou à l'effacement

Dans sa proposition de règlement général pour la protection des données, la Commission européenne apporte une réponse aux préoccupations liées aux spécificités d'Internet relevées ci-dessus en garantissant, notamment, un droit à l'oubli numérique (art. 17 de la proposition de règlement⁽¹⁶⁾⁽¹⁷⁾).

Même s'il ne reprend plus la notion de « droit à l'oubli » dans l'intitulé de la disposition comme c'était le cas dans la proposition de texte provenant de la Commission, l'article 17 tel que modifié par le Parlement prévoit un droit à l'effacement. Ce droit est formulé de la manière suivante :

« Droit à l'effacement »

1. La personne concernée a 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 et elle peut obtenir de tiers l'effacement de tous les liens vers ces données, ou de toute copie ou reproduction de celles-ci, 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 concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19 ;

(16) Cette disposition est reprise dans la présente analyse en tenant compte des modifications adoptées en première lecture par le Parlement européen (voy. 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)).

(17) Voy. A. MANTELERO, « The EU proposal for a general data protection regulation and the roots of the "right to be forgotten" », *C.L.S.R.*, Vol. 29, Issue 3, June 2013, pp. 229 à 235.

c bis) un tribunal ou une autorité réglementaire basé(e) dans l'Union a jugé que les données concernées doivent être effacées et cette décision a acquis force de chose jugée ;

d) les données ont fait l'objet d'un traitement illicite.

2. [...] »⁽¹⁸⁾.

C'est en tant qu'élément de l'autodétermination informationnelle que le droit à l'oubli/l'effacement est abordé, dans cette approche⁽¹⁹⁾.

L'autonomie ou l'autodétermination informationnelle signifie la possibilité de contrôler 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⁽²⁰⁾. 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.

(18) La version de cette disposition telle qu'établie par la Commission européenne différerait relativement peu, puisqu'elle énonçait : « Droit à l'oubli numérique et à l'effacement ».

1. La personne concernée a 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, **en particulier en ce qui concerne des 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, 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 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 présent règlement pour d'autres motifs**. [...] » (Les différences par rapport au texte sont mises en évidence.)

(19) Voy., évoquant également l'autonomie et l'autodétermination en présence de restrictions à apporter à la liberté d'expression, Solove, « The virtues of knowing less: justifying privacy protections against disclosure », 53 *Duke L. J.*, 2003, pp. 967 et 992 : « If the interest of the speaker or listener is defined in terms of self-determination and autonomy, the interest of the harmed individual can be conceptualized in similar terms - as an assault on self-determination and autonomy. There is no clear reason why the autonomy of speakers or listeners should prevail over that of the harmed individuals ».

(20) C. de TERWANGNE, « Internet privacy and the right to be forgotten/right to oblivion », *Revista de Internet, Derecho y Política*, 2012, p. 112, disponible à l'adresse 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. BENYKHELF et P. TRUDEL (éd.), *État de droit et virtualité*, Montréal, Thémis, 2009, pp. 157 à 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, pp. 8 à 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. RIGAUD, *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 », *C.L.S.R.*, 2009, pp. 84 à 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, No. 4, 1989, pp. 675 à 701, disponible à l'adresse <http://scholarship.law.berkeley.edu/facpubs/866>.

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⁽²¹⁾, 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'« autodétermination informationnelle », pour reprendre l'expression énoncée pour la première fois par la Cour constitutionnelle allemande dans sa décision cruciale de 1983⁽²²⁾.

En Europe, cette autodétermination informationnelle a été reconnue et protégée comme un droit, le droit à la protection des données à caractère personnel. Bien évidemment, ce droit à l'autodétermination informationnelle n'est pas absolu. Des intérêts publics ou privés prépondérants doivent être pris en considération, découlant sur de possibles exceptions ou limites au contrôle individuel sur les données.

En tant qu'expression du droit à l'autodétermination informationnelle, le droit à l'oubli est déjà présent sous certaines formes dans le texte de la directive 95/46 relative à la protection des données à caractère personnel. L'article 17 de la proposition de règlement reprend en fait pour l'essentiel ces aspects en n'y ajoutant que quelques éléments. La Cour de justice de l'Union européenne n'aura, pour sa part, pas attendu le vote du texte pour faire surgir de la directive 95/46 un droit au déréférencement ou à la désindexation.

IV

Le droit au déréférencement

Pouvant être considéré comme une des formes du droit à l'oubli, le droit à voir des résultats de recherche retirés de la liste affichée par un moteur de recherche en réponse à une interrogation sur la base du nom d'une personne a été consacré par la Cour de justice dans son arrêt du 13 mai 2014 dont le

(21) 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 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 1^{er} juillet 2008, req. n° 44378/05.

(22) 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 ».

retentissement n'est pas près de faiblir. Il s'agit du droit au déréférencement ou à la désindexation des données.

Le droit à l'oubli en ce sens n'implique pas la suppression des données à la source. Si elles demeurent dans leur contexte initial, les données ne sont pas nécessairement problématiques. On ne désire pas nécessairement leur effacement, mais plutôt l'effacement du résultat du « ratissage » du Web effectué par les moteurs de recherche.

Le pouvoir des moteurs de recherche de rassembler n'importe quelle donnée concernant un individu ciblé, à n'importe quel moment, de n'importe où, gratuitement, sans la moindre formalité administrative et sans que l'interrogateur doive révéler sa propre identité (comme cela peut être le cas lorsque l'on fait des démarches pour consulter des documents dans des administrations publiques, des bibliothèques, des bureaux d'archives...) suscite un danger particulièrement grand. Au vu d'un tel pouvoir des moteurs de recherche en termes d'agrégation de données, il était impératif de reconsidérer avec soin l'équilibre à atteindre entre l'activité de ces derniers, le droit du public à l'information et les droits et intérêts des personnes concernées. C'est ce qu'a été amenée à faire la Cour de justice dans l'affaire *Google Spain*.

La Cour a souligné que l'agrégation des informations publiées sur Internet effectuée par les moteurs de recherche dans le but de faciliter à leurs utilisateurs l'accès à ces informations peut conduire à un aperçu structuré des données relatives à une personne permettant d'établir un profil plus ou moins détaillé de la personne concernée. Ce pouvoir d'agrégation doit être, en outre, combiné à la décontextualisation des données (voy. *supra*, pt II) pour mesurer entièrement le risque spécifique que font naître les moteurs de recherche.

Il convient de citer, en regard de la décision européenne, un arrêt de la Cour suprême américaine⁽²³⁾ prononcé il y a plus de vingt ans mais particulièrement éclairant, où la Cour Suprême a souligné cette nécessité de prise en compte du changement de perspective en présence d'une agrégation de données. 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 survivant 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 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

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

communication « éparpillée » de fragments d'information et la divulgation de l'information dans son ensemble⁽²⁴⁾.

Dans le même sens, dans une autre affaire, 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 »⁽²⁵⁾.

On notera que, dans les lignes directrices qu'il a émises concernant la mise en œuvre de l'arrêt *Google Spain*⁽²⁶⁾, le Groupe de travail « Article 29 » a précisé qu'à ses yeux, ce sont essentiellement les moteurs de recherche généralistes qui suscitent une atteinte aux droits telle qu'évoquée par la Cour. Les moteurs de recherche internes à un site ne correspondent pas à l'hypothèse prise en considération par la Cour dans la mesure où ils ne produisent pas les mêmes effets⁽²⁷⁾.

Les différents aspects du droit au déréférencement mis en évidence par la Cour de justice seront présentés dans les développements ultérieurs consacrés aux éléments pertinents du régime de protection des données qui fondent un tel droit (voy. *infra*, pt VI.B).

On signalera toutefois ici que, d'après les autorités européennes de protection des données, le droit au déréférencement doit valoir plus largement que ce que la Cour n'a dit. Il doit de la sorte valoir pour l'ensemble des noms de domaines (incluant donc les adresses .com), et non être limité aux seuls noms de domaines rattachés à l'Union européenne⁽²⁸⁾.

(24) « 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.)

(25) 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).

(26) Groupe de travail « Article 29 » relatif à la protection des données, 26 novembre 2014, « Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 », WP 225.

(27) *Ibid.*, § 18 : « Search engines included in web pages do not produce the same effects as "external" search engines. On the one hand, they only recover the information contained on specific web pages. On the other, and even if a user looks for the same person in a number of web pages, internal search engines will not establish a complete profile of the affected individual and the results will not have a serious impact on him. Therefore, as a rule the right to de-listing should not apply to search engines with a restricted field of action, particularly in the case of search tools of websites of newspapers ».

(28) *Ibid.*, § 20.

V

Le droit à l'oubli en cas de traitement de données basé sur le consentement de la personne concernée : le droit à l'oubli en tant que droit au repentir et à changer d'avis

Tel que formulé à l'article 17 de la proposition de règlement européen, le droit à l'oubli/l'effacement recouvre deux situations différentes :

- celle où le traitement des données est basé sur le consentement de la personne concernée (ce pt V) ;
- et celle où le traitement des données repose sur un autre fondement que le consentement (*infra*, pt VI).

L'article 17 de la proposition de règlement reconnaît aux personnes concernées 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⁽²⁹⁾. L'article 17 stipule néanmoins que ce retrait peut être considéré comme faisant partie du droit à l'oubli/l'effacement. Par-dessus tout, il apporte un complément d'information quant à l'effet du retrait en termes d'effacement des données (art. 17, § 1^{er}) ou d'utilisation restreinte de celles-ci (art. 17, § 4).

Ainsi, lorsqu'elle retire son consentement de départ, la personne concernée est en droit d'obtenir du responsable du traitement qu'il efface les données à caractère personnel la concernant et cesse ou fasse cesser toute diffusion de ces données. Elle peut, en outre, dans la version du texte adoptée en première lecture par le Parlement, obtenir de tiers l'effacement de tous les liens vers les données problématiques, ou de toute copie ou reproduction de celles-ci.

Ce droit à revenir sur ce que l'on a émis et diffusé et à changer d'avis est particulièrement important dans le contexte d'Internet. Il est précieux lorsque, comme dans la vie ordinaire, on en vient à regretter ce qu'on a exprimé ou diffusé grâce à l'interactivité du Web. De telles situations sont malheureusement fréquentes quand l'expression est spontanée et impulsive, comme c'est souvent le cas sur les sites de réseaux sociaux.

Le repentir ou les changements d'avis surviennent aussi souvent à l'égard d'informations ou de photos partagées à un moment de la jeunesse de leur émet-

(29) L'article 7, § 3, de la proposition de règlement prévoit déjà : « 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 ».

teur. 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 comme immatures, irresponsables, incorrectes ou inconvenantes.

Or, dans la réalité, il s'avère très difficile de réaliser cet exercice sain de nettoyage des stupidités de son passé⁽³⁰⁾. 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 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 »⁽³¹⁾.

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, « [s]i je poste quelque chose en ligne, devrais-je avoir le droit de le retirer ? Je pense que la plupart d'entre nous sommes 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⁾.

VI

Le droit à l'oubli lorsque l'information est traitée/diffusée à l'initiative d'un tiers

A. La mise en balance des intérêts

1. LA RÉOLUTION DES CONFLITS DE DROITS ET INTÉRÊTS

Dans les cas où l'information se rapportant à un individu est traitée ou, plus spécifiquement, est diffusée à l'initiative d'un tiers, les intérêts de la personne concernée, protégés par le droit à l'oubli, entrent en conflit avec d'autres

(30) 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 (*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 », disponibles à l'adresse <http://www.europe-v-facebook.org/EN/Complaints/complaints.html>. Voy. égal. B. VAN ALSENOY, J. BALLEET, 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) 2, pp. 65 à 79.

(31) 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.

(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).

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. 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.⁽³³⁾. Et l'on doit aussi impérativement tenir compte de l'obligation légale de conserver certaines données à des fins de sécurité publique.

En matière de droits de l'homme, la réponse juridique classique 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 tel 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.

2. LES CRITÈRES DE LA RÉSOLUTION DES CONFLITS

Le temps est le premier critère pour résoudre le conflit de droits et d'intérêts.

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 pour le public à être publiés. L'intérêt est 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 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.

(33) 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 à http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_fr.pdf.

La jurisprudence de la Cour européenne des droits de l'homme a mis en évidence des exceptions à ceci. Le droit à l'information garde en effet la primauté, en dépit de l'écoulement du temps :

- en fonction de la nature des faits en cause⁽³⁴⁾ ;
- en fonction de la contribution de l'information en cause à un débat d'intérêt général ;
- 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⁽³⁵⁾.

L'intérêt historique et l'intérêt public, la nature des faits et la personne en cause doivent donc également être pris en considération pour résoudre le conflit entre le droit à l'oubli et le droit à l'information.

Le Groupe de travail « Article 29 » a, pour sa part, élaboré quelques critères de résolution du conflit de droits et intérêts en tenant compte de l'expérience de terrain acquise par les différentes autorités nationales de protection des données⁽³⁶⁾. Ces critères viennent compléter ou éclairer ceux issus de la jurisprudence de la Cour de Strasbourg. Ils sont destinés à aider les autorités de contrôle lors de l'examen des demandes de déréférencement.

3. EXEMPLE DES ARCHIVES DE PRESSE SUR INTERNET. CRITÈRES POUR LA MISE EN BALANCE : ACTUALITÉ, INTÉRÊT HISTORIQUE ET INTÉRÊT PUBLIC

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.

(34) Voy., sur le même critère retenu aux États-Unis, *Briscoe v. Reader's Digest Association, Inc.* 4 Cal. 3d 529 (1971), cité par A. MANTELERO, « The EU proposal for a general data protection regulation and the roots of the "right to be forgotten" », *C.L.S.R.*, Vol. 29, Issue 3, June 2013, pp. 229 à 235 : « The court distinguished between cases in which, by reason of the nature of the facts ("so unique as to capture the imagination of all"), an individual whose name is fixed in the public's memory "never becomes an anonymous member of the community again" and the different cases in which "[...] the only public "interest" that would usually be served is that of curiosity" ».

(35) Sur ces critères, voy. not. Cour eur. D.H., *Osterreichischer Rundfunk*, 7 mars 2007, §§ 61 et s. ; *Axel Springer AG c. Allemagne* [Gr. Ch.], 7 février 2012, req. n° 39954/08, §§ 90 à 95 ; *Haldimann e.a. c. Suisse*, 24 février 2015, req. n° 21830/09, §§ 50 à 55.

(36) Groupe de travail « Article 29 » relatif à la protection des données, 26 novembre 2014, « Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 », *WVP* 225.

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 pouvant s'y attacher. Au titre de cet intérêt public, on peut ranger également l'intérêt pédagogique.

Par définition, les archives des journaux ne sont plus supposées présenter une quelconque valeur d'actualité. Pour ce qui est de leur valeur historique, il faut notamment prendre en compte le fait que d'autres sources d'information existent ou non. Si l'on considère les 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⁽³⁷⁾, 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 »⁽³⁸⁾.

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

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

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 pt VII « 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 scientifiques ou historiques, notamment). Ou le résultat de la mise en balance pourrait être l'exigence que des informations additionnelles soient liées aux données (p. ex., un avertissement ou le point de vue de la personne concernée). La conclusion devrait toujours être atteinte au cas par cas.

On a vu avec l'affaire *Google Spain*, que l'action privilégiée par les particuliers contrariés par ce qui circule sur leur compte sur le Net ne visait pas nécessairement l'effacement des données problématiques du site qui les diffuse, mais s'adresse plutôt, sans doute guidée par un certain pragmatisme, aux moteurs de recherche en vue d'obtenir le déréférencement des informations litigieuses. Cependant cet effacement des listes de résultats demande tout autant qu'une mise en balance des intérêts contradictoires soit effectuée afin de décider de l'effacement ou du maintien des données dans la liste. On verra aux points VI.B.2 et VI.B.3. ci-après les éclaircissements que la Cour de justice a apportés dans l'affaire *Google Spain* sur pareil exercice de mise en balance à l'égard de l'activité d'un moteur de recherche.

On citera, dans la ligne de cet arrêt, une affaire jugée à la fin de l'année 2014 par le Tribunal de grande instance de Paris⁽³⁹⁾, qui illustre également la mise en balance des droits et intérêts en jeu. L'affaire concerne le maintien de données relatives à une condamnation pour escroquerie, dans les résultats affichés par Google en réponse à une interrogation portant sur le nom de la dame visée par la condamnation. Dans son ordonnance de référé, le tribunal signale qu'« [i]l convient d'apprécier si les motifs que M^{me} M. présente au soutien de sa demande tenant à sa situation particulière caractérisent des raisons prépondérantes et légitimes prévalant sur le droit d'expression et d'information ». Le tribunal estimera que deux éléments font pencher la balance en faveur de la suppression de l'information de la liste de résultats : le temps écoulé depuis la condamnation, étant donné que celle-ci a été prononcée plus de huit ans auparavant, et le fait que la condamnation ne figure pas sur le bulletin n° 3 du casier judiciaire, reprenant les seuls éléments de l'état pénal des personnes accessible à des tiers.

Il convient d'avoir à l'esprit que le problème des archives de presse 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

(39) Trib. gr. inst. Paris, réf., 24 novembre 2014, *Marie-France M. c. Google France et Google Inc.*, et Trib. gr. inst. Paris, réf., 19 décembre 2014, *Marie-France M. c. Google France et Google Inc.*, disponibles sur <http://www.legalis.net>.

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.

B. Les éléments du droit à l'oubli issus de la législation de protection des données

1. L'OBLIGATION DE SUPPRIMER DES DONNÉES À CARACTÈRE PERSONNEL DÉCOULANT DU PRINCIPE DE FINALITÉ

Il existe une 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 »⁽⁴⁰⁾. 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.

2. LE DROIT À L'EFFACEMENT DES DONNÉES

a. L'ARTICLE 12, B), DE LA DIRECTIVE 95/46

Le droit à l'effacement de données à caractère personnel est instauré dans l'actuel article 12, b), de la directive 95/46 qui prévoit que toute personne concernée a

(40) Art. 6, § 1^{er}, e), de la directive 95/46.

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 : « 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 au chapitre précédent et on verra dans le point VI.B.3 qui suit 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 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.

b. LES CAS ÉLARGIS DE TRAITEMENT NON CONFORME : NON-RESPECT DES EXIGENCES DE QUALITÉ DES DONNÉES, NON-RESPECT DES HYPOTHÈSES DE LÉGITIMITÉ DES TRAITEMENTS

La Cour de justice, dans l'affaire *Google Spain*, a apporté un remarquable éclairage sur la portée de ce droit à l'effacement. Elle a précisé que, si la non-conformité d'un traitement de données pouvait résider dans le caractère incomplet ou inexact des données, exemples qui sont repris explicitement à l'article 12b, on peut envisager d'autres situations dans lesquelles le traitement est non conforme, étant donné que la disposition introduit ces exemples par « notamment »⁽⁴¹⁾.

Ainsi, selon la Cour, l'article 12b permet aussi à la personne concernée de demander l'effacement de données qui la concernent en cas de non-respect des conditions de licéité des traitements touchant à la qualité des données. Ces conditions sont énoncées à l'article 6 de la directive 95/46 aux termes duquel les données doivent être « adéquates, pertinentes et non excessives ». La Cour a en ce sens précisé que le caractère incompatible du traitement des données « peut résulter non seulement du fait que ces données sont inexactes, mais, en particulier, aussi du fait qu'elles sont inadéquates, non pertinentes ou excessives au regard des finalités du traitement, qu'elles ne sont pas mises à jour ou qu'elles sont conservées pendant une durée excédant celle nécessaire, à moins que leur conservation s'impose à des fins historiques, statistiques ou scientifiques »⁽⁴²⁾.

(41) C.J.U.E., arrêt du 13 mai 2014, *Google Spain et Google Inc.*, précité, § 70.

(42) *Ibid.*, § 92.

Ces qualités des données s'évaluent au regard des finalités pour lesquelles les données sont traitées, mais la Cour a ajouté que l'évaluation se fait également au regard du temps qui s'est écoulé⁽⁴³⁾. Il se peut donc que des informations qui étaient pertinentes à la base se révèlent ne plus l'être ou être devenues excessives par la suite, eu égard à l'ensemble des circonstances du cas considéré.

C'est précisément ce qui a été observé dans l'affaire *Google Spain* à l'égard de certaines informations apparaissant dans la liste de résultats du moteur de recherche. Dans cette affaire, ce n'est pas la pertinence des informations qui était en cause, vu que les données doivent être pertinentes au regard de la finalité du moteur de recherche. Or, cette finalité consistant à recenser tout le contenu du Web au moment d'une demande et à indiquer à l'internaute le contenu correspondant à sa demande, on ne peut considérer un résultat de recherche se rapportant à l'objet de la demande comme non pertinent. Par contre, un résultat peut se révéler excessif, dans la mesure où, tout pertinent qu'il soit, il porte excessivement atteinte aux droits et intérêts de la personne concernée par rapport à l'intérêt que son traitement présente pour le responsable du traitement ou pour autrui. Et cette excessivité peut n'apparaître qu'après l'écoulement d'un certain laps de temps.

Le caractère non conforme d'un traitement de données peut aussi découler du non-respect des conditions de licéité des traitements énoncées à l'article 7 de la directive 95/46 et portant sur les hypothèses de légitimation des traitements de données⁽⁴⁴⁾. Tout traitement de données doit reposer sur une des hypothèses énoncées dans cette disposition pour être jugé admissible. En outre, c'est pour toute la durée pendant laquelle il est effectué que la base de légitimation du traitement doit rester valable⁽⁴⁵⁾.

D'après la Cour de justice, c'est du motif visé à l'alinéa f) que relève le type de traitement effectué par l'exploitant d'un moteur de recherche⁽⁴⁶⁾. Aux termes de cette disposition, un traitement de données est permis lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les libertés et les droits fondamentaux de la personne concernée. La Cour a souligné que « l'application dudit article 7, sous f), nécessite ainsi une pondération des droits et des intérêts opposés en cause dans le cadre de laquelle il doit être tenu compte de l'importance des droits de la personne concernée résultant des articles 7 et 8 de la Charte »⁽⁴⁷⁾.

Il faut donc procéder à une pondération des intérêts. En particulier, l'importance des droits à la vie privée et à la protection des données personnelles, droits garantis aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, doit être prise en compte lors de cette pondération.

(43) *Ibid.*, § 93.

(44) *Ibid.*, § 70.

(45) *Ibid.*, § 95.

(46) *Ibid.*, § 73.

(47) *Ibid.*, § 74.

On verra au point suivant que l'invocation du droit d'opposition, droit figurant également dans la panoplie offerte aux personnes concernées, conduit aussi à une mise en balance des droits et intérêts en jeu.

Les droits à la vie privée et à la protection des données peuvent être atteints « significativement »⁽⁴⁸⁾ par les résultats obtenus à la suite d'une requête effectuée à partir du nom d'un individu dans un moteur de recherche, car la liste de résultats offre « 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 »⁽⁴⁹⁾. L'atteinte potentielle est encore démultipliée si l'on prend en compte l'importance de la place et du rôle joué aujourd'hui par Internet et par les moteurs de recherche ainsi que le rayonnement lié aux caractéristiques techniques du réseau des réseaux, conférant à une liste de résultats « un caractère ubiquitaire »⁽⁵⁰⁾.

Ces constats ont conduit la Cour de justice à la conclusion que l'issue de la mise en balance des droits et intérêts en jeu dans le cadre d'une activité de moteur de recherche était en principe favorable à la personne concernée et devait donc conduire au déréférencement des données en cause. D'après la Cour, l'intérêt économique de l'exploitant d'un moteur de recherche, pas plus que le droit du public à l'information, ne justifie en principe, sous réserve de quelques exceptions⁽⁵¹⁾, l'atteinte grave qui est susceptible de découler de l'affichage de certains résultats de recherche⁽⁵²⁾.

Réaliser une mise en balance afin de vérifier la conformité d'un traitement avec l'hypothèse de légitimité reposant sur l'article 7, f), de la directive revient à procéder à un exercice semblable à celui auquel invite la mise en œuvre du droit d'opposition consacré à l'article 14 de la directive. Ce le sera plus encore lorsque le droit d'opposition tel que consacré par l'article 19 de la proposition de règlement sera d'application (voy. le pt VI.B.3 *infra*). La pondération à effectuer dans le cadre du droit d'opposition devrait toutefois permettre de tenir compte de manière plus spécifique de toutes les circonstances entourant la situation concrète de la personne concernée⁽⁵³⁾.

3. LE DROIT D'OPPOSITION AU TRAITEMENT DES DONNÉES

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⁽⁵⁴⁾.

(48) *Ibid.*, § 80.

(49) *Ibid.*, § 80.

(50) *Ibid.*, § 80.

(51) Ces exceptions sont exposées au point suivant.

(52) *Ibid.*, §§ 81 et 97.

(53) *Ibid.*, § 76.

(54) 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.

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⁽⁵⁵⁾.

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 par rapport à 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 des raisons prépondérantes et légitimes. Dans la version votée par le Parlement européen en première lecture le 12 mars 2014, elles ne doivent même plus se rapporter à la situation particulière de la personne concernée. En cela, le texte diffère de celui proposé par la Commission fin janvier 2012⁽⁵⁶⁾. Pour le Parlement, en outre, lorsqu'un traitement de données a pour fondement le seul intérêt du responsable du traitement ou du destinataire des données (hypothèse prévue à l'art. 6, f.), en compensation, le droit d'opposition doit pouvoir s'exercer « sans frais, à tout moment et sans autre justification, à titre général ou à toute fin spécifique ».

Par ailleurs, le considérant 56 affirme clairement qu'« [i]l 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 impérieuses 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.

La situation où il revient au responsable du traitement de prouver que son intérêt à poursuivre le traitement des données est supérieur à celui des personnes concernées correspond à la situation découlant de l'arrêt *Google Spain* où la Cour a tranché dans le sens d'une primauté de principe des droits de la personne concernée, sous réserve que le responsable d'un moteur de recherche démontre un intérêt supérieur à la poursuite de la sélection et de l'affichage des données. Selon la Cour de justice, en effet, vu la gravité potentielle de l'atteinte, les droits à la vie privée et à la protection des données garantis aux articles 7 et 8 de la Charte des droits fondamentaux doivent en principe prévaloir sur l'intérêt écono-

(55) Art. 14, § 1^{er}, b), de la directive 95/46.

(56) L'article 19.1 de la proposition de règlement émise par la Commission 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 ». (En italique, les éléments disparaissant dans la version adoptée par le Parlement en première lecture.)

mique du moteur de recherche et sur l'intérêt du public à trouver l'information lors d'une recherche basée sur le nom d'une personne.

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 les intérêts en faveur du droit à l'oubli. Cela signifie qu'une inévitable mise en balance de ces intérêts devra avoir lieu.

Ce qui a été exposé au point précédent concernant les traitements de données liés à l'activité d'un moteur de recherche sur Internet intervient de la même manière ici.

Des balises ont été récemment proposées pour faciliter et uniformiser au sein de l'Union européenne l'exercice de mise en balance des droits et intérêts. Comme indiqué plus haut (voy. *supra*, pt VI.A.2), le Groupe de travail « Article 29 » a, en effet, publié le fruit de son travail de concertation visant à indiquer des critères destinés à aider les autorités de contrôle lors de l'examen des demandes de déréférencement⁽⁵⁷⁾. Les critères en question devraient en fait pouvoir être appliqués également pour l'exercice du droit d'opposition à l'égard d'informations diffusées sur un site source et non pas seulement à l'égard de listes de résultats élaborées par un moteur de recherche. Il s'agit notamment de vérifier si on est ou non en présence de données factuelles dont l'exactitude peut être mesurée, de tenir compte du rôle public ou non de la personne concernée, du fait que celle-ci est mineure ou non, de la nature de l'information (données sensibles ou ordinaires), du risque que l'information fait courir à la personne concernée, etc.⁽⁵⁸⁾.

VII

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

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

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 d'effacer/supprimer les données (disparition des données elles-mêmes) ou de les anonymiser (disparition des éléments identifiants⁽⁵⁹⁾).

(57) Groupe de travail « Article 29 » relatif à la protection des données, 26 novembre 2014, « Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 », WP 225.

(58) Sur l'exercice difficile qui attend les moteurs de recherche et les autorités de contrôle, voy. E. DERREYNE et R. ROBERT, « L'arrêt "Google Spain" : une clarification de la responsabilité des moteurs de recherche... aux conséquences encore floues », *R.D.T.I.*, 2015.

(59) Il convient d'être conscient des limites des processus d'anonymisation au vu des pratiques croissantes de brassage et de croisement de grandes quantités de données qualifiées d'anonymes, et des risques existants de « désanonymisation ». Ces limites et problèmes ne peuvent faire l'objet de plus de développements dans la présente contribution.

L'article 17, § 1^{er}, de la proposition de règlement garantit à la personne concernée par les données 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 devrait donc avoir le droit de demander que ses données à caractère personnel soient supprimées et non pas seulement rendues inaccessibles, comme c'est la pratique développée par certains réseaux sociaux.

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

Le droit à l'oubli peut induire par ailleurs l'obligation de verrouiller les données. Le terme « verrouiller » a été pointé comme étant équivoque par les auteurs de la proposition de règlement⁽⁶⁰⁾ qui lui ont préféré l'expression « limiter le traitement », qui n'est malheureusement pas vraiment 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. Le Parlement européen propose de préciser en outre que la limitation du traitement des données doit se faire « de manière à ce qu'elles ne soient pas soumises aux manipulations usuelles d'accès aux données et de traitement des données exécutées par le responsable du traitement et qu'elles ne puissent plus être modifiées »⁽⁶¹⁾.

D'autres résultats de l'exercice du droit à l'oubli, différents de ceux issus de dispositions explicites et mentionnés ci-dessus, pourraient également être envisagés et permettraient de mieux respecter le principe de proportionnalité :

- l'accès restreint aux données : dans certains cas, le problème découle de la diffusion publique des données, et non du traitement interne des données. La personne concernée pourrait, en pareil cas, souhaiter arrêter la publication des données, mais accepter que les données continuent d'être conservées et utilisées en interne par le responsable du traitement, et communiquées de façon restreinte ;
- d'autres formes de publicité ou l'arrêt de certaines formes de diffusion : cette solution 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 (une personne a consenti, par exemple, à être filmée et accepte

(60) 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" ».

(61) Art. 17, § 4, de la 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]).

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) ;

- la suppression de tout lien vers les données et de tout référencement pour les moteurs de recherche : il se peut, à l'instar de ce qui s'est passé dans l'affaire *Google Spain*, que la personne concernée veuille agir contre la décontextualisation et serait simplement heureuse de voir ses données déréférencées, désindexées, tout lien vers elles étant supprimé. Ce serait là l'instrument adéquat contre la décontextualisation 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 ;
- l'adjonction d'une information supplémentaire aux données (p. ex., un avertissement ou le point de vue de la personne concernée) ;
- l'anonymisation des données n'apparaît explicitement dans le texte légal qu'associée au respect du principe de finalité. Or il peut se présenter d'autres cas où la personne concernée n'a pas l'intention de voir ses données effacées ; ne plus être associée aux données pourrait lui suffire. L'anonymisation des données pourrait être une réponse adéquate à une telle aspiration.

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 (p. ex., en matière de sécurité publique, 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. L'information en aval des demandes d'effacement de données

« Afin de renforcer le "droit à l'oubli numérique" dans l'environnement en ligne »⁽⁶²⁾, l'article 17, § 2⁽⁶³⁾, de la proposition de règlement émise par la Commission 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

(62) Considérant 54 de la proposition de règlement.

(63) L'article 17, § 2, de la proposition de règlement énonce que, « [l]orsque 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 ».

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 »⁽⁶⁴⁾.

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, la principale étant que 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.

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, il 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. 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⁽⁶⁵⁾.

Il convient de relever que la praticabilité du devoir d'information tel qu'imaginé dans la proposition de texte de la Commission est déjà fortement contestée⁽⁶⁶⁾. Il semble clair que les obligations additionnelles insérées dans le texte du Parlement 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⁽⁶⁷⁾. Et

(64) Considérant 54 de la proposition de règlement.

(65) Art. 7.2 : « Lorsque le responsable du traitement visé au paragraphe 1 a rendu publiques les données à caractère personnel sans aucune justification fondée sur l'article 6, paragraphe 1, il prend toutes les mesures raisonnables pour procéder à l'effacement de ces données, y compris par des tiers, sans préjudice de l'article 7.7. Le responsable du traitement informe la personne concernée, lorsque cela est possible, des mesures prises par les tiers concernés ». (En italique, les éléments ajoutés ou modifiés dans la version adoptée par le Parlement en première lecture) 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, amendement n° 121.

(66) Voy. not. l'opinion du Contrôleur européen à la protection des données, *op. cit.*, §§ 146 et 147.

(67) 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/>.

entrer en contact avec toutes ces personnes pourrait se révéler vraiment difficile, voire même impossible. La possibilité de solutions techniques est envisagée 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, de plus, 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)⁽⁶⁸⁾.

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, confondu avec le droit à l'effacement tel que perçu dans la directive 95/46, 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. Cela étant, on a vu que la Cour de justice a invité à une interprétation large du champ d'application du droit à l'effacement. Elle a clairement établi que c'est en présence de tout traitement non conforme des données qu'on pouvait invoquer ce droit et pas seulement pour corriger des données incomplètes ou inexactes.

VIII

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

En réponse aux nouveaux développements de services Internet et à la situation problématique induite par les spécificités d'Internet relevées au point 2 de cette contribution, la même proposition a été formulée dans différents cercles

(68) 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, amendements n°s 35 et 147.)

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⁽⁶⁹⁾. 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 »⁽⁷⁰⁾. La Vice-Présidente de la Commission européenne, Viviane 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 »⁽⁷¹⁾.

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

Ce système de radiation automatique 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, § 1^{er}, de la CEDH. Elles ne devraient pas être conservées sans procéder à une analyse très stricte de la nécessité de cette conservation par rapport aux exigences démocratiques⁽⁷²⁾.

(69) 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/D1, 22 juin 2011, pp. 1 et s., § 85.

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

(71) 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).

(72) Cour eur. D.H., *Rotaru c. Roumanie*, 4 mai 2000, 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.

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⁽⁷³⁾. Il permet aux utilisateurs d'attacher une date d'expiration digitale aux images enregistrées sur des sites de réseaux sociaux comme Facebook.

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 seulement 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

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 ;
- le droit de ne pas voir en permanence rappelé 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 ou parce que c'est non conforme aux règles de protection des données ;

(73) <http://www.x-pire.de/index.php?id=6&L=2>.

- le droit de refuser la décontextualisation 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.

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⁽⁷⁴⁾, 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. 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.

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 souci en soi, 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 a tenté de lui donner et son usage par les individus, confrontés à des difficultés liées à leurs données en circula-

tion 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.

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 ci-dessus 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) ou sur le droit d'effacer le lien électronique vers les données (dans le but de lutter efficacement contre la décontextualisation des données tout en les maintenant accessibles dans les cercle et contexte originaux), ou sur le droit de restreindre la diffusion (p. ex., sur des réseaux sociaux).

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 des données en aval des traitements qu'il effectue. Il a plus de chances 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.

(74) Art. 17 de la proposition de règlement, précité.