UCL
Université catholique de Louvain

Faculté de droit et de criminologie (DRT)

Le droit à l'oubli numérique dans le droit de l'Union européenne

Consécration prétorienne et législative

Mémoire réalisé par
Maxime BESÈME

Promoteur
Marc FALLON

Année académique 2015-2016
Master en droit

Plagiat et erreur méthodologique grave

Le plagiat entraîne l'application des articles 87 à 90 du règlement général des études et des examens de l'UCL.

Il y a lieu d'entendre par « plagiat », l'utilisation des idées et énonciations d'un tiers, fussent-elles paraphrasées et quelle qu'en soit l'ampleur, sans que leur source ne soit mentionnée explicitement et distinctement à l'endroit exact de l'utilisation.

La reproduction littérale du passage d'une oeuvre, même non soumise à droit d'auteur, requiert que l'extrait soit placé entre guillemets et que la citation soit immédiatement suivie de la référence exacte à la source consultée.*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

Table des matières

Introduction

« *L'oubli est une quête juridique aussi difficile à atteindre que le bonheur* »
Jean-Michel Brugière[1]

Il y a quelques mois à peine, l'Union européenne se dotait d'un nouvel instrument juridique ayant entre autres pour objectif de répondre aux nouveaux défis lancés par l'apparition de l'Internet. En effet, la mémoire sans limite de ce juge virtuel intemporlel met aujourd'hui en péril certains de nos droits fondamentaux, tels que la vie privée et la protection des données à caractère personnel. Avec le temps, nous avons pris conscience des dérives auxquelles mène la conservation infinie de nos données. Nos pairs et ceux qui leur succéderons sont et seront à présent en mesure de juger un grand nombre d'informations nous concernant[2]. Le monde numérique a ainsi changé notre perception de la mémoire, propulsant les internanutes dans un univers parallèle qu'ils ne contrôlent plus et dans lequel « oublier » n'existe plus. Les traces et les ombres que nous laissons sur la toile sont à chaque instant susceptibles de re-faire surface. Seule une intervention extérieure semble pouvoir garantir ce qui, hier, résultait encore d'un simple processus psychologique[3].

C'est dans ce contexte particulier que le droit européen a progressivement élaboré le désormais célèbre « droit à l'oubli ». D'abord consacré par la Cour de justice de l'Union européenne, il fait aujourd'hui l'object d'une disposition portant son nom dans un nouveau règlement 2016/679.

Cette étude a pour but d'aborder le droit à l'oubli sous sa forme actuelle et de présenter ce qu'il sera demain. A cette fin, elle revient tout d'abord sur les différentes terminologies que l'on rencontre habituellement dans la littérature académique et sur les fondements ayant conduit à la consécration de ce droit nouveau. Elle analyse ensuite un ensemble de questions pratiques permettant d'élaborer, étapes par étapes, le shéma de raisonnement qu'il convient à une personne concernée d'appréhender avant de demander la mise en œuvre de son droit. A qui puis-je demander la suppression de mes données ? Quand et comment cela s'effectue-t-il ? Quels sont les obstacles possibles ? Enfin, elle passera en revue les principales nouveautés du droit à l'oubli établies par le règlement 2016/679.

---

[1] J.-M. BRUGUIÈRE, « Le droit à l'oubli numérique, un droit à oublier », *D. (D.S.)*, 2014, p. 202.
[2] V. MAYER-SCHÖNBERGER, *Delete : The Virtue of Forgetting in the Digital Age*, Princeton, Princeton
[2] V. MAYER-SCHÖNBERGER, *Delete : The Virtue of Forgetting in the Digital Age*, Princeton, Princeton University Press, 2009.
[3] J. DUPONT-LASSALE, « Beaucoup de bruit pour rien ? La précarité du droit à l'oubli numérique consacré par la Cour de justice de l'Union européenne dans l'affaire Google Spain », *Rev. trim. D.H.*, 2015, p. 989.

Chapitre 1er : Notion de droit à l'oubli et son application au contexte numerique : taxinomie et terminologie

« Droit à l'oubli », « droit à l'effacement », « droit au déréférencement » ou « à la désindexation », « droit à l'oubli numérique ». La doctrine, le juge et le législateur européens, notamment, se sont tous trois penchés sur la notion générale de « droit à l'oubli », et ont chacun apporté leur lot de nouveautés dans la terminologie employée en la matière. La littérature académique s'est maintes fois essayée à proposer une approche holistique de ces concepts sans être encore parvenue à s'accorder sur des définitions claires de ces différentes expressions[4]. Le nouveau règlement général de protection des données[5] permettra certainement à l'avenir de résoudre ces difficultés terminologiques de par la consécration en son sein d'un « droit à l'oubli » défini et encadré. Cependant, c'est sur base de la directive 95/46 relative à la protection des données personnelles que la matière est actuellement réglée. Les sections suivant cette courte introduction font état des différents développements proposés jusqu'à aujourd'hui et tentent de replacer les termes dans leur contexte afin d'en faire bon usage. Notre propos se focalisera sur l'emploi de ces notions dans l'environnement qu'est celui des institutions européennes. Certaines références au droit national des États membres seront cependant parfois nécessaires.

Section 1ère : Les différentes « facettes » du droit à l'oubli

Le terme général de « droit à l'oubli » couvre au moins deux domaines disposant chacun d'un champ d'application qui lui est propre, même si certains recoupements sont inévitables[6]. Nous verrons que depuis quelques années, une troisième facette de ce droit, ou plutôt une

[4] N. XANTHOULIS, « Conceptualising a Right to Oblivion in the Digital World: A Human Rights-Based Approach », p. 8, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2064503 (14 mars 2016).
[5] Règl. (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/47/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, du 4 mai 2016, p. 1.
[6] Elise Defreyne le présente comme étant un droit « multi-facettes ». *Voy*. E. DEFREYNE, « Le droit à l'oubli et les archives journalistiques », *R.D.T.I*, 2013, p. 3.

« facette 2*bis* », fort similaire à la seconde mais née du besoin de l'adapter au contexte numérique et de l'internet, est en cours d'élaboration[7].

Le droit à l'oubli…

L'expression « droit à l'oubli » pouvant être indifféremment employée pour l'une ou l'autre des trois dimensions exposées ci-dessous, les problèmes dus à la terminologie sont récurrents[8]. Pour pallier à cette difficulté, la doctrine anglophone oppose le plus souvent les termes de « *right to forget* » à ceux de « *right to be forgotten* », désignant respectivement « *la revitalisation d'un fait du passé* », soit le droit à l'oubli judiciaire, et « *le droit à l'effacement des données* »[9]. Néanmoins, d'autres termes tels que « *right to oblivion* » ou « *right to erasure* » sont aujourd'hui abondamment présents dans les articles et ouvrages traitant du sujet, et maintiennent malgré tout une certaine forme de confusion dans l'emploi du vocabulaire[10].

Le droit à l'oubli numérique…

Dans la doctrine francophone, « le droit à l'oubli numérique », est l'expression utilisée initialement par la Commission à l'article 17 de la proposition de règlement général de protection des données publiée en janvier 2012[11], lequel a pour but de remplacer la directive 95/46 actuelle. De nombreux auteurs font également usage de cette expression lorsqu'ils désignent « l'adaptation du droit à l'oubli au contexte numérique », soit la troisième « facette » que nous exposerons ci-dessous.

Le droit à l'effacement…

« Le droit à l'effacement » est la dénomination finale retenue par le Parlement et le Conseil pour ce même article 17 du nouveau règlement général. Nous ne ferons usage de ce terme que lorsque nous examinerons la nouvelle disposition en détail.

---

[7] C. DE TERWANGNE, « Internet Privacy and the Right to Be Forgotten/Right to Oblivion », *Revista de Internet, Derecho y Política*, 2012, p. 110.

[8] E. DEFREYNE, « Le droit à l'oubli et les archives journalistiques », *op. cit*., p. 78 ; R.H. WEBER, « The Right to Be Forgotten : More Than a Pandora's Box ? », *J.I.P.I.T.E.C.*, 2011, p. 120.

[9] R.H. WEBER, « The Right to Be Forgotten : More Than a Pandora's Box ? », *op.cit*., p. 121.

[10] Pour un aperçu des différentes terminologies utilisées par la doctrine anglophone, *voy*. E. DEFREYNE, « Le droit à l'oubli et les archives journalistiques », *op. cit*., p. 78 et les références citées en notes de bas de page.

[11] 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 et à la libre circulation de ces données (règlement général sur la protection des données), *C.O.M*. (2012) 11 final, p. 57. *Voy*. également le commentaire de P. DE HERT et V. PAPKONSTANTINOU, « The proposed data protection Regulation replacing Directive 95/46/EC : A sound system for the protection of individuals », *Computer Law & Security Review*, 2012, pp. 130-142.

Aux formules que nous venons d'aborder, il convient encore de présenter « le droit au déréférencement » ou « à la désindexation », droit prétorien consacré par la Cour de Justice de l'Union européenne dans son arrêt du 13 mai 2014, dit « arrêt *Google Spain* »[12]. Il permet aux individus de demander à ce que certaines données les concernant, obtenues par la saisie de mots clefs (leur nom et prénom par exemple) dans un moteur de recherche, soient retirées de la liste des résultats affichés. L'information n'est donc pas supprimée à la source, mais elle est rendue pratiquement introuvable.

Difficultés terminologiques…

Malgré l'existence de termes « spécifiques » pour désigner les différentes facettes du droit à l'oubli, force est de constater que la littérature académique ne s'en soucie guère, probablement du au fait que la notion elle-même est encore vague. Récemment, Grégory Voss et Céline Castets-Renard ont publié une étude proposant une taxonomie internationale reprenant les différentes formes du droit à l'oubli[13]. Malheureusement, étant rédigée en anglais, celle-ci s'adapte difficilement aux subtilités linguistiques de la langue française. Elle a toutefois le mérite de rassembler dans un seul document les différentes définitions envisagées par la doctrine européenne et internationale.

§ 1er : Le droit à l'oubli judiciaire.

Le premier domaine couvert fait référence au droit subjectif reconnu aux personnes ayant fait les frais d'une « *évocation fautive* [dans la presse] *d'anciens faits criminels pour lesquels elles ont été condamnées*[14] ». Il s'agit donc de permettre à quiconque de demander à ce que des informations diffusées dans la presse, replaçant son passé judicaire sur le devant de la scène, soient retirées[15]. Pour être qualifiée de « fautive », la diffusion des informations doit être appréciée au regard de son contexte factuel (l'information est-elle utile à la poursuite d'un intérêt contemporain ? contribue-t-elle à un débat public ? jouit-elle d'un caractère historique ? etc.[16]). Ce « droit à l'oubli du passé judicaire » a été reconnu par la jurisprudence

[12] C.J.U.E., 13 mai 2014 (Google Spain S.L. et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, http://www.curia.europa.eu (16 novembre 2014).
[13] C. CASTETS-RENARD et W.G. VOSS, « Proposal for an International Taxonomy on the Various Forms of the « Right to Be Forgotten » : A Study on the Convergence of Norms », *Colorado Technology Law Journal*, 2016, n°14, pp. 281-344.
[14] E. DEFREYNE, « Le droit à l'oubli et les archives journalistiques », *op. cit*., p. 3.
[15] J. ROSEN, « Symposium Issue. The Right To Be Forgotten », *Stanford Law Review Online*, Vol. 64, 2012, p. 88.
[16] E. DEFREYNE, « Le droit à l'oubli et les archives journalistiques », *op. cit*., p. 3.

dans différents États membres sur base du droit à la vie privée ou des droits de la personnalité, comme le droit à la dignité ou à la réputation[17]. Bien que partageant de nombreux points communs avec le droit à l'oubli dans le contexte du numérique[18], nous ne faisons ici que le mentionner. Il ne fera dès lors pas l'objet de notre attention dans la suite de notre étude.

§ 2 : Le droit au retrait des données à caractère personnel

Le second domaine, plus récent, fait allusion au « *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*[19] ».

Ces informations, ou *données*, sont définies par la directive 95/46 comme étant « *toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à son identité physique, physiologique, psychique, économique, culturelle ou sociale*[20] ».

L'idée est de permettre aux individus de ne pas être indéfiniment confrontés à leur passé[21] en leur offrant la possibilité de contrôler activement des données les concernant, accessibles à des tiers, et qu'ils estiment ne plus être pertinentes[22]. Cela suppose concrètement de pouvoir demander au responsable du traitement des données à ce que les données en question soient effacées, mais également de demander d'en interdire l'accès et l'utilisation aux tiers[23].

---

[17] C. DE TERWANGNE, « Internet Privacy and the Right to Be Forgotten/Right to Oblivion », *op. cit*., p. 111 ; A. CASSART et J.F. HENROTTE, « Droit de l'homme numérique. Introduction générale aux droits de l'homme numérique – Droit à l'oubli : une réponse à l'hypermnésie numérique », 2012, p. 5, www.uianet.org/sites/.../HENROTTE%20JeanFrançois%20Droit%20à%20l'oubli.pdf (17 novembre 2015).

[18] Le droit à l'oubli judiciaire s'est également adapté au contexte du numérique, la presse se servant de plus en plus de moyens modernes tel que l'Internet comme canal de diffusion. Cependant, l'objet visé reste, malgré tout, la publication d'articles de presse (électronique) ressassant le passé judiciaire des individus. Comme nous le verrons plus loin, le droit à l'oubli adapté au contexte du numérique, tel que nous l'entendons, s'écarte de ce cas spécifique et vise plutôt les données diffusées sur internet par des particuliers (et non pas par la presse).

[19] C. DE TERWANGNE, « 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 », *in Enjeux européens et mondiaux de la protection des données personnelles* (sous la dir. de A. GROSJEAN), Bruxelles, Larcier, 2016, p. 246 (C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit.*).

[20] art. 2, a), de la directive 95/46.

[21] *Ibid*., p. 246.

[22] B.-J. KOOPS, « Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right To Be Forgotten in Big Data Practice », *SCRIPTed*, Vol. 8, n° 3, 2011, p. 4.

[23] N. XANTHOULIS, « Conceptualising a Right to Oblivion in the Digital World : A Human Rights-Based Approach », *op. cit*., p. 9.

Certains auteurs suggèrent également qu'il soit possible de demander l'anonymisation des données en supprimant les éléments identifiants[24].

Parfois présenté comme un « *intérêt légitime à oublier et à se faire oublier*[25] » plutôt que comme un véritable « droit » au sens légal du terme, le concept envisagé sous cet angle trouve ses racines dans le régime de la protection des données personnelles[26], et, plus précisément, dans la mise en œuvre des principes de proportionnalité et de « limitation de la finalité[27] ». Ce dernier présuppose que les données personnelles doivent être traitées loyalement, dans un but « *déterminé, légitime, et transparent*[28] ». Dans le cadre du droit européen, la directive 95/46/CE relative à la protection des données personnelles[29] reste, à ce jour, le cadre législatif juridiquement contraignant le plus pertinent[30], bien que d'autres dispositions, notamment issues des droits fondamentaux, viennent également encadrer la matière[31].

Enfin, certains intègrent à ce second versant du droit à l'oubli le « droit d'opposition », lequel permet de demander à « bloquer l'utilisation des données[32] ». Pour Gabriela Zanfir, cela signifie, en pratique, que ni les tiers ni la personne concernée n'auront plus accès à l'information bloquée, bien que celle-ci restera stockée auprès du responsable des données qui ne sera plus autorisé à la traiter d'aucune façon[33].

---

[24] C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit*., p. 267 ; E. DEFREYNE, « Le droit à l'oubli et les archives journalistiques », *op. cit*., p. 84.

[25] A. ROUVROY, « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information », version augmentée du chapitre paru dans *La sécurité de l'individu numérisé – Réflexions prospectives et internationales*, Paris, L'Harmattan, 2008, p 25.

[26] C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit*., p. 246 ; C. DE TERWANGNE, « Internet Privacy and the Right to Be Forgotten/Right to Oblivion », *op. cit*., p. 113.

[27] *Idem*, p. 114.

[28] *Idem*, p. 114.

[29] Dir. (CE) n° 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E*., L. 281, du 23 novembre 1995, p. 31.

[30] Le nouveau règlement 2016/679 ne sera applicable qu'à partir du mois de mai 2018.

[31] Nous présenterons ces autres sources dans le cadre de l'historique du droit à l'oubli. *Voy*. à cet égard la section 2 du premier chapitre.

[32] S. SIMITIS, *Collected courses of the Academy of European Law*, Vol. VIII, n° 1, The Hague, Kluwer Law International, 1997, p. 130.

[33] G. ZANFIR, « Tracing the Right to Be Forgotten in the Short History of Data Protection Law : The New Clothes of an Old Right », *in Reforming European Data Protection Law* (sous la dir. de S. GUTWIRTH, P. DE HERT et R. LEENES), Dordrecht, Heidelberg, New York, London, Springer, 2015, p. 243.

§3 : Le droit à l'oubli adapté au contexte du numérique

Le développement croissant du web 2.0[34], les disparités liées à la transposition de la directive 95/46/CE dans les droits nationaux des États membres, l'insécurité juridique qui en découle, la complexité des règles relatives aux transferts internationaux de données, etc., sont autant de raisons invoquées par la Commission européenne[35] pour justifier la nécessité d'adapter le régime actuel de protection des données au contexte numérique. Dans une communication datant de janvier 2010 annonçant le lancement prochain du processus de révision de la directive 95/46, la Commission a présenté 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*[36] ».

Comme le souligne Cécile de Terwangne, « *l'autodétermination informationnelle* » et « *le rôle déterminant de la volonté de l'individu* » sont au cœur de cette version moderne du droit à l'oubli[37]. Ce dernier prend d'avantage en compte les nouveaux moyens de communication et offre un cadre plus conforme à la tendance croissante de diffusion d'informations en tout genre sur les réseaux sociaux. De même, il s'est adapté aux nouveaux systèmes d'accès à l'information que sont les moteurs de recherche, lesquels permettent aujourd'hui de rassembler un grand nombre d'informations décontextualisées en très peu de temps et à moindre frais.

Section 2 : Le droit à l'oubli dans les premières lois relatives à la protection des données personnelles en Europe

Le droit à l'oubli ou « droit à l'effacement », tel qu'aujourd'hui établi à l'article 17 du nouveau règlement européen relatif à la protection des données à caractère personnel[38], est le fruit d'une longue et complexe construction juridique débutée dans les années 70 et 80[39], lors

[34] E. MONTERO et Q. VAN ENIS, « Les métamorphoses du droit à l'oubli », *R.G.D.C.*, 2016, p. 248.
[35] 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 donnés à caractère personnel dans l'Union européenne », *C.O.M.* (2010) 609 final, pp. 3-4.
[36] *Ibid*., p. 9.
[37] C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit*., p. 247.
[38] Règl. (UE) n° 2016/679 (*voy*. n° 2).
[39] G. GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, Heidelberg, New York, Dordrecht, London, Springer, 2014, p. 21.

de l'adoption des premières lois nationales régissant la protection des données en Europe. Allemands et Français furent précurseurs en la matière. L'influence de leurs législations respectives est largement reconnue et ces dernières servirent de modèle en Europe[40]. Cependant, d'autres législations européennes contribuèrent tout autant à la construction du droit à l'oubli. Nous dressons ici un portrait global et succinct de ces lois avant-gardistes et pionnières[41], conçues, à l'époque, afin de répondre aux problèmes suscités par les premiers systèmes de traitement de l'information « modernes ».

En Allemagne…

En Allemagne, la *Bundesdatenschutzgesetz*, entrée en vigueur en 1977[42], et succédant à la première loi nationale adoptée par la Chancellerie d'État du Land de Hesse[43], stipulait déjà que « *chacun a le droit, en vertu de la présente loi* […] (4) : *à l'effacement des données sauvegardées le concernant, si leur conservation était inadmissible, ou – outre le droit au verrouillage des données – lorsque les conditions de stockage initialement prévues ne sont plus valables*[44] ».

Comme il vient d'être suggéré, le § 27 (3)[45] de la même loi de l'époque permettait également à la personne concernée de choisir entre l'effacement ou *le verrouillage des données*[46]. Dès lors, si le droit à l'oubli n'était pas explicitement consacré, celui-ci prenait déjà la forme d'un « droit à l'effacement » ou, à tout le moins, d'un « droit au blocage » des données[47].

En France…

[40] E.A. SHOOR, « Narrowing the Right to be Forgotten : Why the European Union needs to amend the Proposed Data Protection Regulation », *Brooklyn Journal of International Law*, 2014, Vol. 39, n° 1, p. 493.
[41] Les différentes lois nationales exposées ci-après ont été mises en évidence par Gabriela Zanfir. *Voy*. G. ZANFIR, « Tracing the Right to Be Forgotten in the Short History of Data Protection Law : The New Clothes of an Old Right », *op. cit*., pp. 239-241. Dans la mesure du possible, nous nous sommes efforcés de les référencer de façon similaire à la méthode belge, tout en tenant compte des particularités propres au référencement de certaines lois étrangères.
[42] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG) du 27 janvier 1977, *BGBl*, 1, 1er février 1977, p. 201.
[43] Il s'agit également de la première loi au monde en matière de protection des données personnelles. *Voy*. G. GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *op. cit*., p. 56.
[44] Traduit de l'allemand par nous : « §4 *Rechte des Betroffen*: *Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf […] (4) : Löschung der zu seiner Person gespeicherten Daten, wenn ihre Speicherung unzulässig war oder - wahlweise neben dem Recht auf Sperrung - nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung*. » Le terme « Löschung » ou « effacement » est mentionné pas moins de 12 fois dans la loi fédérale allemande de l'époque.
[45] Dans les pays germanophones, le symbole « § » correspond au terme « article » en français.
[46] § 27 (3) de la loi de la loi allemande de 1977.
[47] B. SIEMEN, *Datenschutz als europäisches Grundrecht*, Berlin, Duncker & Humblot, 2006, p. 35.

En France, l'article 36 de la loi relative à l'informatique, aux fichiers et aux libertés[48], stipulait que « *le titulaire du droit d'accès peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées*[49] *les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite* ». L'article 38 ajoutait que « *si une information a été transmise à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par la Commission* ».

Au Royaume-Uni…

Au Royaume-Uni, l'article 24 du *Data Protection Act* de 1984[50], intitulé « *rectification et effacement*[51] », permettait aux personnes concernées de soumettre un formulaire de demande à la Cour afin de réclamer la rectification ou l'effacement de données erronées, ou des données détenues par un utilisateur (entendez « le responsable des données ») et contenant « *l'expression d'une opinion qui apparaît à la Cour comme étant basée sur des données erronées*[52] ».

Seule la Cour était donc autorisée à permettre l'effacement de données, lesquelles devaient être jugées incorrectes. Ces dernières pouvaient toutefois avoir été fournies aussi bien par des tiers que par la personne concernée elle-même[53]. Il s'agissait donc d'un « droit à l'effacement » très limité plutôt que d'un véritable « droit à l'oubli ».

Aux Pays-Bas…

Enfin, *het Wet Persoonsregistraties*, entrée en vigueur en 1989 aux Pays-Bas, accordait aux personnes concernées le droit de demander, par écrit, à l'utilisateur des données (à nouveau, entendez « responsable de traitement »), de rectifier, compléter ou effacer des données si l'accès à celles-ci avait révélé qu'elles étaient erronées, ou incomplètes pour les finalités pour lesquelles elles étaient conservées, ou non pertinentes, ou apparaissent, après examen, contraire à une disposition légale[54]. La loi allait même plus loin et exigeait des utilisateurs des données qu'ils communiquent aux tiers à qui ils avaient sciemment fournis les données les

[48] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[49] Souligné par nous.
[50] 1984 c. 35.
[51] Traduit par nous : « *Rectification and Erasure* ».
[52] Section 24 (1) *in fine*, du Data Protection Act 1984.
[53] Section 24 (2).
[54] Article 33, §1er, de la loi hollandaise.

corrections (rectifications, ajouts, effacements) effectuées sur ces celles-ci. Cela était vrai pour tous les tiers ayant traité les données dans l'année précédant la demande de la personne concernée. Cette dernière pouvait également fournir une liste reprenant les tiers qui, à son avis, avaient pris connaissance de ses données[55].

Des principes communs…

Le droit à l'effacement n'est donc pas nouveau. Les législateurs nationaux en Europe avaient, dès les années 70 et l'avènement des nouvelles technologies, saisi la nécessité d'introduire dans leurs législations une sorte de « droit de contrôle » sur les données à caractère personnel. Bien qu'ayant connu des débuts difficiles, notamment eu égard à la mise en œuvre de ce « droit à l'oubli moderne[56] » et aux définitions éparses des finalités pour lesquelles celui-ci fut introduit dans les législations européennes[57], certains points communs pouvaient déjà être dégagés. Ainsi, le droit à l'effacement n'était le plus souvent possible que lorsque les données étaient erronées ou qu'elles n'étaient pas nécessaires à l'accomplissement des finalités pour lesquelles elles avaient été collectées, ou encore parce qu'elles avaient été rassemblées de façon « illégale ».

De même, l'obligation d'informer les tiers ayant eu accès aux données de ce que celles-ci ont fait l'objet d'une correction, était déjà au cœur de certaines législations nationales. Comme nous le verrons plus loin, il s'agit d'une obligation centrale permettant l'effectivité du droit à l'effacement.

Section 3 : Les sources du droit à l'oubli dans l'Union européenne

§1er : La directive 95/46/EC

La directive 95/46/EC[58] est actuellement le principal instrument européen, juridiquement contraignant, établissant un socle commun en matière de protection des données entre les

[55] Article 35 de la loi. *Voy*. A.C.M. NUGTER, *Transborder Flow of Personal Data within EC*, Amsterdam, Springer, 1990, pp. 145 et s.
[56] Par opposition à un droit à l'oubli « contemporain », tel que définit aujourd'hui dans le contexte du numérique et de l'internet.
[57] L.A. BYGRAVE, *Data Protection Law. Approaching its Rationale, Logic and Limits*, The Hague, London, New York, Kluwer Law International, 2002, p. 8.
[58] Dir. (CE) n° 95/46.

différents États membres. Lors de son adoption, le législateur européen entendait poursuivre la réalisation du marché intérieur (via, notamment, l'instauration d'un cadre légal pour la libre circulation des données personnelles[59]), et protéger davantage les droits et libertés fondamentaux des individus[60]. Cependant, de l'aveu même de la Commission, la perspective économique et celle du marché intérieur ont prévalu en tant que fondement juridique de la directive[61]. Ce n'est qu'après l'adoption de la Charte des droits fondamentaux de l'Union européenne — laquelle consacre spécifiquement et de manière autonome[62] le droit à la protection des données personnelles dans son article 8 — que le second objectif originellement présenté (la protection des droits et libertés fondamentaux des individus) fut ramené à sa juste place[63].

Si le droit à l'oubli n'est pas explicitement mentionné dans la directive, cette dernière comporte des dispositions à travers lesquelles l'exercice de ce droit est possible[64]. On parle d'un « *droit latent dans un certain nombre de dispositions phares*[65] ».

§2 : La jurisprudence de la Cour de Justice

Jusqu'à récemment, la Cour de Justice de l'Union européenne n'avait pas eu l'occasion de se prononcer sur la reconnaissance ou non d'un droit à l'oubli numérique. Dans un arrêt du 13 mai 2014[66], rendu en grande chambre sur question préjudicielle, elle entérine définitivement l'existence du principe et met fin à l'ambiguïté qui subsistait jusque-là[67].

---

[59] *Voy*. considérant n°3 de la directive 95/46 : « *considérant que l'établissement et le fonctionnement du marché intérieur dans lequel* […] *la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés* ».

[60] P. DE HERT et S. GUTWIRTH, « Data Protection in the Case Law of Strasbourg and Luxembourg : Constitutionalisation in Action », *in Reinventing Data Protection ?* (sous la dir. de P. DE HERT, C. DE TERWANGNE, S. GUTWIRTH et S. NOUWT), Dordrecht, Springer, 2009, p. 8.

[61] Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), *C.O.M.* (2003) 265 final, p. 4.

[62] A. ARAMAZANI, « Le droit à l'oubli et internet », *R.D.T.I.*, 2011, p. 40.

[63] P. DE HERT et S. GUTWIRTH, « Data Protection in the Case Law of Strasbourg and Luxembourg : Constitutionalisation in Action », *op. cit*., p. 9.

[64] A. ARAMAZANI, « Le droit à l'oubli et internet », *op. cit*., p. 39.

[65] M. BOIZARD, A. BLANDIN, C. CORGAS-BERNARD, G. DEDESSUS LE MOUSTIER et al., Le droit à l'oubli [Rapport de recherche], Mission de recherche Droit et Justice, 2015, http://www.gip-recherche-justice.fr/publication/le-droit-loubli-2/, (12 octobre 2015).

[66] C.J.U.E., 13 mai 2014 (Google Spain S.L. et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, http://www.curia.europa.eu (16 novembre 2014).

[67] D. HEYWOOD et C. REES, « The right to be forgotten or the principle that has been remembered », *Computer Law & Security Review*, 2014, p 577.

Contexte factuel…

Un ressortissant espagnol, Mr Costeja Gonzáles, souhaitait d'une part voir supprimées, ou à tout le moins modifiées, certaines informations publiées dans un journal espagnol, « La Vanguardia Ediciones », toujours disponibles sur le site du quotidien, et mentionnant son nom en lien avec une vente aux enchères immobilière. Cette dernière avait été pratiquée à son encontre en 1998, en recouvrement de dettes de sécurité sociale qui avaient depuis lors été payées. D'autre part, il demandait que ces informations soient supprimées ou occultées dans la liste des résultats obtenus après saisie de son nom sur le moteur de recherche Google.

Le journal et Google[68] ayant tous deux refusé d'accéder à sa demande, Mr Costeja Gonzáles s'est alors tourné vers l'Agence espagnole de protection des données (Agencia Española de Protección de Datos, ou « AEPD »), laquelle a refusé d'ordonner au quotidien la suppression des données, mais a, en revanche, accueilli la réclamation dirigée contre Google Spain et Google Inc. En effet, l'AEPD estimait que les exploitants de moteurs de recherche étaient soumis à la législation en matière de protection des données, « *étant donné qu'ils réalisent un traitement de données pour lequel ils sont responsables et qu'ils agissent en tant qu'intermédiaires de la société d'information*[69] ».

Considérant que les liens vers les pages *web* concernées du journal espagnol étaient susceptibles de porter atteinte au droit de la protection des données et au droit à la dignité au sens large dont jouit Mr Costeja Gonzáles, droits qui engloberaient également la simple volonté de la personne intéressée que ces données ne soient pas connues par des tiers, l'AEPD a dès lors ordonné à Google le retrait des liens de son moteur de recherche.

Le groupe américain avait alors introduit un recours auprès de l'Audiencia Nacional pour contester cette décision. Le tribunal espagnol, avant de statuer, a saisi la Cour de plusieurs questions préjudicielles relatives à l'interprétation de la directive 95/46/CE, notamment sur la question du champ d'application territorial de celle-ci ainsi que sur l'existence d'un « droit à l'oubli numérique ».

[68] Google estimait que la demande devait être introduite auprès de la maison mère, aux Etats-Unis.
[69] C.J.U.E., 13 mai 2014 (Google Spain S.L. et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 17.

Commentaires…

Tout d'abord, bien que consacré dans le cadre d'une affaire liée au passé judicaire de la personne concernée, le droit à l'oubli établi par la Cour doit pouvoir également s'appliquer aux situations telles que celles couvertes par le droit à l'oubli numérique de manière globale[70]. Cela serait faussement interpréter l'intention de la Cour que de restreindre son enseignement aux seules demandes d'effacement de données liées à des antécédents avec la justice.

Il faut également relevé que la question posée ne portait pas sur la suppression de données en tant que telles, mais bien sur la possibilité de faire disparaître des données dans une liste de résultats obtenus après avoir introduit un nom dans la barre de saisie d'un moteur de recherche. Autrement dit, comme l'a souligné à mainte reprises la doctrine francophone[71], la question portait davantage sur l'existence d'un « droit au déréférencement » ou à la « désindexation » de données que sur l'existence d'un « droit à l'oubli numérique » de façon plus générale. Cependant, les auteurs s'accordent à dire qu'il s'agit « *d'une des formes du droit à l'oubli*[72] ».

De plus, la Cour laisse le soin aux autorités nationales de protection des données d'adopter les mesures appropriées sur base d'une analyse au cas-par-cas. Une marge de manœuvre est donc encore laissée aux États membres qui sont seuls habilités à trancher les litiges sur base de la transposition de la directive dans leur droit national[73].

Enfin, vous verrons au travers de l'analyse des différents éléments qui constituent le droit à l'oubli, que l'arrêt *Google Spain* laisse encore en suspend un certain nombre de questions auxquelles il conviendra, dans la mesure du possible, d'apporter des réponses[74].

---

[70] I. COFONE, « Google v. Spain : A Right To Be Forgotten ? », *Chicago-Kent Journal of International and Comparative Law*, 2015, Vol. 15, p. 5.
[71] C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit*.,p. 253.
[72] *Ibid.,* p. 253.
[73] *Voy*. par exemple, pour une application de l'arrêt *Google Spain* aux Pays-Bas : S. KULK et F. ZUIDERVEEN BORGESIUS, « Freedom of Expression and Right to Be Forgotten Cases in the Netherlands After Google Spain », *E.D.P.L*., 2015, Vol. 2, pp. 113-124.
[74] A ce propos, *voy*. par exemple M. DOUGLAS, « Questioning the Right To Be Forgotten », *Alternative Law Journal*, 2015, Vol. 40, n° 2, pp. 109-112 ; J. KERR, « What is a Search Engine ? The Simple Question the Court of Justice of the European Union Forgot to Ask and What It Means for the Future of the Right to be Forgotten », *Chicago Journal of International Law*, 2016, Vol. 17, n°1, pp. 217-243.

Chapitre 2 : Contre qui peut-on invoquer le droit à l'oubli ?

Section 1ère : Champ d'application territorial de la directive 95/46[75]

Avant de poursuivre avec l'analyse des dispositions pertinentes en matière de droit à l'oubli et relatives au champ d'application matériel de la directive, il nous semble essentiel d'analyser le champ d'application spatial de celle-ci. En effet, avant d'identifier le responsable de traitement, faut-il encore déterminer si ce dernier est soumis aux règles établies par la directive[76]. Or, dans l'environnement particulier que représente Internet, la question de *l'applicabilité* du droit est une chose délicate. Lorsque le responsable de traitement est situé au sein de l'Union européenne, le droit européen s'applique naturellement au travers des lois nationales le transposant[77]. Mais force est de constater qu'un grand nombre de services numériques, tels que les moteurs de recherche et les réseaux sociaux, brassant la majorité des données susceptibles de faire, un jour, l'objet d'une demande d'effacement, sont issus d'États tiers, tels que les Étas-Unis par exemple[78]. Comment permettre alors à un individu « d'oublier » ou de « faire oublier » une information publique disponible partout dans le monde ? Nous n'analyserons ici que la solution apportée par la Cour.

§1er : Le responsable de traitement dispose d'un établissement secondaire sur le territoire d'un État membre

L'article 4, § 1er, a), de la directive 95/46 dispose que lorsque « *le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire* [d'un] *État membre* », les règles nationales de cet État, transposant le droit européen, doivent

[75] La question du champ d'application territorial de la directive étant relativement vaste, nous nous focaliserons sur les éléments essentiels nous permettant, d'une part, d'identifier les difficultés liées à l'application de la directive dans l'espace, et, d'autre part, d'apporter, dans la mesure du possible, des solutions à ces problèmes.

[76] Étonnement, il n'est en revanche pas nécessaire d'analyser le champ d'application spatial de la directive au regard de la personne concernée. Comme le soulève Bruno Hardy, celle-ci s'applique à tout citoyen, qu'il soit européen ou non. *Voy*. B. HARDY, « Application dans l'espace de la directive 95/46/CE : la géographie du droit à l'oubli », *Rev. trim. dr. europ*., 2014, p. 880.

[77] Sur la question de la transposition des directives dans le droit national et les critères d'applicabilité des directives européennes, *voy*. S. PRECHAL, *Directives in EC Law*, Oxford, Oxford University Press, 2005, pp. 180 à 216.

[78] Le siège social de Google Inc. est établi à Mountain View, en Californie.

s'appliquer. Sur base de cette disposition, la Cour de justice de l'Union européenne a estimé que « *lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants* [d'un] *État membre* », il faut alors considérer que l'établissement ainsi créé[79] effectue un traitement de données à caractère personnel « *dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire de* [cet] *État membre*[80] ». Pour autant, l'établissement dont il est question ne doit pas nécessairement avoir été préalablement qualifié de « responsable de traitement » et le traitement ne doit pas nécessairement avoir lieu sur le territoire de l'un des États membres de l'Union[81].

Au travers de son jugement, la Cour a ouvert la porte à l'application du droit européen en matière de protection des données à des entités établies dans des États tiers, tels que les États-Unis en l'espèce, et disposant d'un établissement secondaire sur le sol européen[82]. Son argumentation se base essentiellement sur deux éléments : d'une part, le lien étroit qui existe entre l'établissement et la société mère responsable du traitement[83] et, d'autre part, la nécessité de rendre effectifs les droits consentis par la directive, spécialement vis-à-vis des droits fondamentaux[84].

Dans la mise-à-jour de son opinion 8/2010 relative au droit applicable, le G29 a interprété l'arrêt de la Cour comme permettant d'appliquer la directive à des sociétés établies en dehors de l'Union européenne, dont le modèle économique serait basé sur l'offre de « services gratuits[85] » sur le territoire de l'Union, et financés par le traitement de données à caractère

[79] En l'espèce, il s'agissait de la société *Google Spain*, filiale de Google Inc. Les activités du moteur de recherche de Google ont été considérées comme étant effectuées *dans le cadre des activités* de Google Spain, établissement secondaire situé en Espagne.
[80] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 60.
[81] L. MOEREL, « The long arm of EU data protection law : Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide ? », *International Data Privacy Law*, 2011, p. 29.
[82] Dans son arrêt *Weltimmo*[82], postérieur à *Google Spain*, la Cour considère qu'un responsable de traitement dispose d'un établissement établi dans un État membre si ce dernier peut être qualifié « *d'installation stable* » et qu'il exerce une « *activité effective et réelle, même minime* » dans le cadre du traitement des données personnelles dont il est question. *Voy*. C.J.U.E., 1er octobre 2015 (Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság), C-230/14, point 41.
[83] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 56. Dans ce cas-ci, le lien est un lien économique, *Google Spain* pourvoyant aux revenus de Google Inc.
[84] *Ibid*., points 53, 54 et 58.
[85] Le G29 n'exclut pas que sur base d'un examen au cas par cas, d'autres modèles économiques puissent également tomber dans le champ d'application de la directive. *Voy*. Groupe de travail « Article 29 » sur la

personnel, à des fins de prospection par exemple. Cette possibilité dépendrait néanmoins du cas d'espèce et du rôle joué par l'établissement secondaire[86]. Il ajoute également que lorsqu'une société dispose de plusieurs établissements dans différents États membres, celle-ci devra se conformer aux droits nationaux de chacun de ces États. A nouveau, une analyse au cas par cas devra déterminer si les activités de ces établissements sont en lien étroit avec celles de la maison mère, responsable du traitement[87].

§2 : Le responsable de traitement ne dispose pas d'un établissement secondaire sur le territoire d'un État membre

La Cour n'a pas encore été amenée à se pronconer sur cette situation. Néanmoins, il est fort à parier que les éléments pertinents présentés dans le paragraphe suivant doivent pouvoir s'appliquer à ce contexte-ci[88].

§3 : Le droit international public

Malgré les explications fournies par la Cour et le G29, le schéma complet du raisonnement permettant d'aboutir à l'application extraterritorial du droit de l'Union nécessite encore un détour par le droit international public[89]. A cet égard, deux principes en particulier, issus de la coutume, retiennent notre attention : le principe de territorialité et la théorie des effets[90]. Afin toutefois de concentrer notre attention sur le droit à l'oubli en tant que tel et la manière dont celui-ci doit être mis œuvre par les États membres, nous nous contenterons de les exposer sans plus de détails[91].

---

protection des données, « Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain », 16 décembre 2015, 176/16/EN WP 179 update, p. 7. Voy. également F.H. CATE, C. KUNER, O. LYNSKEY, C. MILLARD et D.J.B. SVANTESSON, « When two worlds collide : the interface between competition law and data protection », *International Data Privacy Law*, 2014, p. 248.

[86] Groupe de travail « Article 29 » sur la protection des données, « Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain », 16 décembre 2015, 176/16/EN WP 179 update, p. 5.

[87] *Ibid.,* pp. 6-7.

[88] Voy. J. AUSLOOS , A. KUCZERAWY et B. VAN ALSENOY, « Search engines after Google Spain : internet@liberty or privacy@peril? », *op. cit*., p. 8.

[89] Christopher Kuner estime en effet que lorsque la question est liée à la mise en œuvre d'une décision de justice relative à la protection des données personnelles, celle-ci doit être traitée au regard du droit international public et non pas privé. *Voy*. C. KUNER, « Data protection Law and International Jurisdiction on the Internet (Part 1) », *International Journal of Law and Information Technology*, 2010, pp. 181-183.

[90] Issu de la doctrine anglophone: « *effects doctrine* ». *Voy*. à ce sujet J. KLABBERS, *International Law*, Cambridge, Cambridge University Press, 2013, p. 96.

[91] Pour une analyse plus approfondie du rôle du droit international public dans la sphère de la concrétisation du droit à l'oubli, *voy*. notamment D.J.B. SVANTESSON, « The Extraterritoriality of EU Data Privacy Law — Its

Ainsi, sur base du premier principe, chaque État a le droit d'intervenir lorsque les circonstances mettent en cause des personnes, des matières ou des situations opérant sur leur territoire[92]. Dans l'affaire *Google Spain*, c'est l'établissement de Google Inc., en tant que responsable de traitement, qui, via sa filiale espagnole, donne le droit à la Cour d'appliquer la directive. Lokke Moerel considère à ce propos que « *le principe de territorialité est* […] *observé par l'article 4, §1er, a), par le fait que le traitement des données est virtuellement connecté au territoire de l'UE* » via les activités de l'établissement établi dans un État membre[93].

Afin de renforcer la déclaration de compétence juridictionnelle de la Cour, certains auteurs plus créatifs soulèvent également l'applicabilité de la théorie des effets[94]. Bien que celle-ci soit généralement pratiquée en matière de droit de la concurrence[95], elle permet à un État d'intervenir à l'égard d'actes perpétrés à l'étranger dès lors que ceux-ci produisent des effets substantiels sur son territoire[96]. C'est expressément ce que semble viser la Cour lorsqu'elle insiste sur la nécessité de protéger les droits et libertés fondamentaux affectés par les activités des moteurs de recherche[97].

Si la décision de la Cour a fait couler beaucoup d'encre, Brendan Van Alsenoy et Marieke Koekkoek rappellent que statuer en sens inverse serait revenu à désavantager grandement les responsables de traitement européens qui, eux, sont déjà soumis à la directive[98].

Theoretical Justification and Its Practical Effect on U.S. Businesses », *Stanford Journal of International Law*, 2014, Vol. 50, n° 1, pp. 54-102 ; M. KOEKKOEK et B. VAN ALSENOY, « Internet and jurisdiction after Google Spain : the extraterritorial reach of the right to be delisted », *International Data Privacy Law*, 2015, pp. 105-120.

[92] U. KOHL, *Jurisdiction and the Internet. Regulatory Competence over Online Activity*, Cambridge, Cambridge University Press, 2010, pp. 89 et s.

[93] L. MOEREL, « The long arm of EU data protection law : Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide ? », *op. cit*., p. 30.

[94] M. KOEKKOEK et B. VAN ALSENOY, « Internet and jurisdiction after Google Spain : the extraterritorial reach of the right to be delisted », *op. cit*., p. 109.

[95] J. KLABBERS, *International Law*, *op. cit*., p. 96.

[96] D.J.B. SVANTESSON, « The Extraterritoriality of EU Data Privacy Law — Its Theoretical Justification and Its Practical Effect on U.S. Businesses », *op. cit*., p. 82.

[97] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 58.

[98] Ces deux auteurs parlent de « *special guest status* » accordé aux responsables de traitement étrangers. *Voy*. M. KOEKKOEK et B. VAN ALSENOY, « Internet and jurisdiction after Google Spain : the extraterritorial reach of the right to be delisted », *op. cit*., p. 113. En sens contraire, Bruno Hardy conclu « *qu'il aurait sans doute été plus opportun de conclure à l'inapplicabilité de la directive* ». *Voy*. B. HARDY, « Application dans l'espace de la directive 95/46/CE : la géographie du droit à l'oubli », *op. cit*., p. 19.

Section 2 : La notion de responsable de traitement

§1er : Considérations générales

Si le droit à la rectification, à l'effacement ou au verrouillage de données est reconnu par la directive 95/46/CE au profit des personnes concernées, encore faut-il savoir à l'encontre de qui est-il possible de le mettre en œuvre. En effet, identifier la personne (physique ou morale) *responsable du traitement* des données[99] n'est pas toujours chose aisée. Celle-ci est définie dans la directive comme étant « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* […][100] ». La doctrine ajoute qu'elle est *« responsable des choix qui président à la définition et à la mise en œuvre des traitements*[101] », quand bien même elle ne disposerait pas matériellement des données en cause[102].

En pratique, si les dispositions permettant la création d'un « droit à l'oubli » étaient relativement faciles à appliquer dans les années 90[103], les difficultés liées à l'internet et aux nouvelles *ICT*[104] ont rendu la tâche plus difficile. L'apparition des réseaux sociaux et des moteurs de recherche en particulier ont exigé de faire preuve d'ingéniosité et d'adapter l'interprétation des règles de droit actuelles à des situations nouvellement crées par l'arrivée d'Internet. Les sections suivantes ont pour but de cerner la notion de « responsable de traitement » à la lumière du contexte numérique tel que nous le vivons aujourd'hui, tout en intégrant les derniers développements apportés par la Cour de Justice de l'Union européenne et le groupe de travail Article 29 sur la protection des données[105]. En raison de leur

[99] L'article 6, §2, de la directive 95/46 dispose clairement « [qu']*il incombe au responsable de traitement d'assurer le respect du paragraphe 1* », lequel énumère les différentes qualités que doivent revêtir les données afin qu'elles puissent être traitées. Sur l'analyse de l'article 6, *voy. infra*. De même, les articles 12 et 14 de la directive font état des obligations qui incombent au « responsable de traitement ». *Voy*. aussi le considérant n°25 de la directive : « *considérant que les principes de la protection doivent trouver leur expression* […] *dans les obligations mises à la charge des personnes, autorités publiques, entreprises, agences ou autres organismes qui traitent des données* […] ».

[100] Art. 2, d), de la directive 95/46.

[101] M.-H. BOULANGER, C. DE TERWANGNE, T. LÉONARD, S. LOUVEAUX, D. MOREAUX et Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.*, 1997, p. 126.

[102] M. WALRAVE, *Privacy Gescand? Direct marketing en de bescherming van de persoonlijke levenssfeer*, Leuven, Universitaire Pers Leuven, 1999, p. 224.

[103] B.-J. KOOPS, « Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right To Be Forgotten in Big Data Practice », *op. cit*., p. 9.

[104] « Technologies de l'information et de la communication », (TIC) transcription de l'anglais « Information and Communication Technologies » (ICT).

[105] Le G29 ou Groupe de travail Article 29 sur la protection des données est un organe consultatif indépendant

importance en termes de cas pratiques, nous limiterons notre exposé aux réseaux sociaux et aux moteurs de recherche[106].

§2 : Les réseaux sociaux

Les réseaux sociaux sont définis par le G29 comme étant des « *plateformes de communications en ligne permettant aux individus de rejoindre ou de créer des réseaux entre utilisateurs partageant des intérêts communs*[107] ». Ils permettent également de « *publier et échanger des informations avec les autres utilisateurs*[108] ». L'un des problèmes majeurs lorsque l'on cherche à identifier le « responsable de traitement » dans un environnement tel que celui des réseaux sociaux, réside donc dans la pluralité des acteurs susceptibles de correspondre à la définition donnée par la directive. N'étant pas à exclure que dans certains cas, et le fournisseur de service, et les utilisateurs du réseau social, soient conjointement responsables[109], ils seront tous deux tenus d'exécuter les obligations qui leur incombent vis-à-vis de la personne concernée[110], ce qui comprend notamment, et sous réserve du régime que nous exposerons plus loin, la rectification, l'effacement ou le verrouillage de données. De même, il est possible qu'une même entité soit soumise à plusieurs régimes juridiques différents[111] car elle cumule plusieurs rôles dans le cadre d'une opération d'ensemble[112].

établi par l'article 29 de la directive 95/46. Composé d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission, il est notamment chargé de contribuer à la mise en œuvre homogène de la directive 95/46 par les États membres (art. 30, §1er, a), de la directive 95/46).

[106] Il nous faut cependant constater que la notion de « responsable de traitement » joue également un rôle déterminant à l'égard d'autres exemples. Il en va ainsi notamment du propriétaire d'un immeuble qui déciderait de faire installer des caméras de surveillance, d'une agence de voyage disposant de toutes les coordonnées de ses clients ou, dans la même idée, de banques, lesquelles disposent également d'un certain nombre de données sensibles.

[107] Groupe de travail « Article 29 » sur la protection des données, « Opinion 5/2009 on online social networking », 12 juin 2009, 01189/09/EN WP 163, p. 3.

[108] Groupe de travail « Article 29 » sur la protection des données, « Opinion 1/2010 on the concepts of controller and processor », 16 février 2010, 00264/10/EN WP 169, p. 21.

[109] L'article 2, d) mentionne expressément la possibilité d'une responsabilité conjointe. *Voy*. également à ce sujet Groupe de travail « Article 29 » sur la protection des données, « Opinion 1/2010 on the concepts of controller and processor », 16 février 2010, 00264/10/EN WP 169, p. 22.

[110] C. KUNER, *European Data Protection Law. Corporate Compliance and Regulation*, 2nd Edition, Oxford, Oxford University Press, 2007, p. 72.

[111] Dans certains cas, lorsque les entités désignées comme « responsables du traitement » sont soumises à des droits différents, par exemple parce qu'ils proviennent de pays différents, peut également se poser la question du droit applicable, faisant alors appel aux règles de droit international privé. A cet égard, *voy*. notemment L.A. BYGRAVE, « European Data Protection – Determining Applicable Law Pursuant to European Data Protection Legislation », *Computer Law & Security Review*, 2000, pp. 254-255, et l'analyse de l'article 4 de la directive 95/46 que nous effectuons plus loin (*cfr. infra*).

[112] M.-L. LAFFAIRE, *Protection des données à caractère personnel*, Paris, Éditions d'Organisation, 2005, p. 91.

Ces considérations nous amènent à distinguer deux situations. La première prend pour exemple la posture d'un utilisateur ayant lui-même téléchargé des données sur le réseau social et souhaitant les voir retirées ou effacées. La seconde part de l'hypothèse qu'un tiers a publié sur ce même réseau des données liées à la personne concernée.

A. L'utilisateur publie lui-même l'information

Lorsqu'un utilisateur publie lui-même une information sur un réseau social (vidéos, photos, opinions, etc.), il doit être en mesure de supprimer lui-même le contenu de cette publication ou de demander au fournisseur de service de supprimer les données[113]. Ce dernier, parce qu'il prodigue les moyens nécessaires au traitement des données des utilisateurs ainsi que tous les services « de base » liés à la gestion de ces moyens (l'enregistrement et la suppression des comptes notamment)[114], et parce qu'il détermine les finalités pour lesquelles ces données sont traitées, est en première ligne au rang de « responsable de traitement ». Ainsi, Facebook[115], Twitter, YouTube, et autres « *SNS providers*[116] » sont légalement tenus, lorsqu'il y a lieu de supprimer une donnée, de prendre les mesures nécessaires afin de répondre à la demande de l'utilisateur.

B. Un tiers a publié l'information

La situation devient rapidement plus complexe lorsqu'un utilisateur publie des informations liées à quelqu'un d'autre, comme des photos ou des vidéos. Dans ce cas, il y a lieu de se demander si cet utilisateur peut également être considéré comme « responsable du traitement ». En effet, l'article 3, § 2, 2e tiret[117], de la directive permet de faire sortir du champ d'application de la directive les traitements de données à caractère personnel

[113] Groupe de travail « Article 29 » sur la protection des données, « Opinion 5/2009 on online social networking », 12 juin 2009, 01189/09/EN WP 163, p. 11, point 3.9.
[114] *Ibid.*, p. 5.
[115] Pour une étude plus approfondie des règles de protection des données appliquées au réseau social « Facebook », *voy*. J.-F. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010, pp. 235-271 ; R. CIAVARELLA et C. DE TERWANGNE, « Online Social Network and Young People's Privacy Protection : The Role of the Right to Be Forgotten », *in Minding Minors Wandering the Web : Regulating Online Child Safety* (sous la dir. de S. VAN DER HOF, B. VAN DEN BERG et B. SCHERMER), The Hague, Springer, 2014, pp. 157-171.
[116] « Social Network Services providers » ou « Fournisseurs de services de réseaux sociaux ».
[117] Cette limitation au champ d'application de la directive est la seule à ne pas être susceptible de dérogation sur base de l'article 13. *Voy*. C.J.U.E., 16 décembre 2008 (*Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*), C-73/07, points 45-47, http://www.curia.europa.eu (14 juin 2016), et le point 125 des conclusions de l'Avocat général.

« *effectué[s] par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques*[118] ». En d'autres mots, si l'utilisateur est à même de prouver que le traitement des données qu'il a publiées sur le réseau social s'exerce dans le cadre « *d'activités exclusivement personnelles ou domestiques* », il ne sera alors pas considéré comme un « responsable de traitement » et ne sera pas soumis aux obligations qui en découlent.

Le G29 tempère cette exception et relève que de plus en plus d'utilisateurs se servent des réseaux sociaux comme plateforme de communication pour une association ou une société[119]. Il considère dès lors que lorsque l'utilisateur « *agit sous le couvert d'une société ou d'une association, ou utilise le réseau social principalement comme une plateforme à des fins commerciales, politiques ou pour des objectifs philanthropiques, l'exception ne s'applique pas*[120] ».

De même, dans son arrêt Lindqvist du 6 novembre 2003[121], la Cour de Justice de l'Union européenne a eu l'occasion de préciser que cette exception visait « *uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet*[122] *de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes*[123] ». L'Avocat général Tizzano avait interprété la notion de manière similaire : « *cette catégorie recouvre uniquement des activités* […] *manifestement privées et confidentielles, destinées à ne pas sortir de la sphère personnelle ou domestique des intéressés*[124] ». Dans un second arrêt, plus récent, la Cour a confirmé sa jurisprudence

[118] La doctrine anglophone parle de « *household exception* » ou « exception domestique ».
[119] Groupe de travail « Article 29 » sur la protection des données, « Opinion 5/2009 on online social networking », 12 juin 2009, 01189/09/EN WP 163, p. 6.
[120] *Ibid*., p. 6, point 3.1.1.
[121] C.J.C.E., 6 novembre 2003 (Bodil Lindqvist), C-101/01, http://www.curia.europa.eu (14 juin 2016).
[122] Zuzanna Warso critique ce point de vue, trop large selon elle. Elle relève qu'avec les moyens modernes, notamment les réglages de confidentialité mis à disposition sur la plupart des interfaces des réseaux sociaux (« *privacy settings* »), les informations publiées sur internet ne sont pas nécessairement accessibles au grand public. Selon elle, l'exception domestique ne devrait pouvoir être soulevée que lorsque le responsable de traitement a fait usage des réglages de confidentialité et a limité l'accessibilité des données à un public restreint (en limitant la visibilité d'une photo à ses seuls amis Facebook par exemple). *Voy*. Z. WARSO, « There's more to it than data protection — Fundamental rights, privacy and the personal/household exemption in the digital age », *Computer Law & Security Review*, 2013, pp. 495-496.
[123] C.J.C.E., 6 novembre 2003 (Bodil Lindqvist), C-101/01, point 47, souligné par nous.
[124] Point 34 des conclusions de l'Avocat général Tizzano rendues sous l'arrêt Bodil Lindqvist. *Voy*. également le commentaire de DE TERWANGNE C., « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *R.D.T.I.*, 2004, p. 88.

antérieure en insistant sur le caractère « *exclusivement personnel*[…] *ou domestique*[…] » que doivent revêtir les activités litigieuses[125].

Ainsi, comme le met en évidence Jean-Philippe Moiny, « *deux critères sont à prendre en compte : la nature de l'activité en cause et le degré d'accessibilité de l'information*[126] ». Dès lors, l'utilisateur ne pourra en fin de compte se prévaloir de « l'exception domestique » que s'il parvient à prouver que l'information a été publiée dans le cadre de sa vie privée ou familiale et qu'elle n'a pas été rendue accessible à un nombre indéfini de personnes, cette dernière condition devant inévitablement tenir compte des paramètres de confidentialité[127] appliqués à la page *web* sur laquelle se trouvent les données en question[128]. Une évaluation *in concreto* et au cas par cas permettra de trancher. Si celle-ci trouvait à ne pas s'appliquer, il serait alors nécessaire de mettre en balance d'une part le droit à l'effacement détenu par la personne concernée, et, d'autre part, le droit à la liberté d'expression de l'utilisateur. Nous verrons cependant que la Cour semble plutôt en faveur du droit à la protection des données personnelles.

Dans le cas contraire, si l'utilisateur peut se prévaloir de « l'exception domestique » et par conséquent ne pas être considéré comme un « responsable de traitement », il nous semble qu'il soit alors possible de se retourner contre le fournisseur de services[129], sur base de la

[125] C.J.U.E., 11 décembre 2014 (František Ryneš c. Úřad pro ochranu osobních údajů), C-212/13, point 30, http://www.curia.europa.eu (14 juin 2016). Dans cette affaire, il s'agissait d'un propriétaire ayant placé une caméra de surveillance devant sa maison afin de dissuader d'éventuels malfrats. Celle-ci couvrait non seulement l'entrée de la maison, mais également le trottoir public ainsi que la maison d'en face. La Cour a jugé que le propriétaire ne pouvait se prévaloir, en l'espèce, de l'exception domestique car la caméra couvrait également des espaces publics. A ce propos, *voy*. le commentaire de O. TAMBOU, « Arrêt Rynes : la vidéo-surveillance et la directive sur la protection des données personnelles », *J.D.E.*, 2015, pp. 107-108. *Voy*. également L. WOODS, « Big Brother's Little Brother ? The scope of the household exception to EU data protection law », 2014, http://eulawanalysis.blogspot.be/2014/07/big-brothers-little-brother-scope-of.html (17 mars 2016).

[126] J.-F. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 251, point 30.

[127] Le G29 considère ainsi que lorsque l'utilisateur est en réseau avec un nombre important d'autres utilisateurs qu'il pourrait même ne pas connaître, il s'agit d'un signe permettant d'écarter potentiellement l'application de l'exception domestique. L'utilisateur serait alors considéré comme « responsable de traitement » au regard de la directive. *Voy*. Groupe de travail « Article 29 » sur la protection des données, « Opinion 5/2009 on online social networking », 12 juin 2009, 01189/09/EN WP 163, p. 6, spéc. point 3.1.1. *in fine*.

[128] J. SAVIRIMUTHU et R. WONG, « All or Nothing : This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet », *John Marshall Journal of Computer & Information Law*, 2008, Vol. 25, p. 260.

[129] Bert-Jaap Koops en doute cependant, arguant qu'en pratique, les différents « responsables de traitement » risquent de se renvoyer la balle, rendant la responsabilité conjointe difficile. *Voy*. B.-J. KOOPS, « Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right To Be Forgotten in Big Data Practice », *op. cit.*, p. 10.

responsabilité conjointe[130]. Une autre solution serait de faire usage de l'article 14, a), de la directive, qui permet à la personne concernée « *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*[131] ».

Nous remarquons cependant qu'en pratique, il n'est pas toujours facile de trouver le responsable de traitement. Par exemple, l'emploi de sites « mirroirs » permet à des tiers de reproduire à l'infini des données contenues sur un site *Web*. Dans ces circonstances, comment retrouver l'ensemble des responsables de traitement ? Il faut dès lors relativiser la portée du droit à l'oubli sous sa forme actuelle.

§3 : Les moteurs de recherche

La question de savoir si un moteur de recherche peut être considéré comme un « responsable de traitement de données publiées sur les pages *Web* source de tiers » a été expressément soulevée devant la Cour de justice de l'Union européenne[132]. Celle-ci a constaté que l'exploitant d'un moteur de recherche « *collecte* [des informations publiées sur internet] *qu'il extrait, enregistre et organise par la suite dans le cadre de ses programmes d'indexation, conserve sur ses serveurs et, le cas échéant, communique à et met à disposition de ses utilisateurs sous forme de listes des résultats de leurs recherches*[133] ».

Elle est ainsi arrivée à la conclusion que « *c'est l'exploitant du moteur de recherche qui détermine les finalités* […] *du traitement de données à caractère personnel qu'il effectue, lui-même, dans le cadre de* [son activité] *et qui doit, par conséquent, être considéré comme le responsable de ce traitement*[134] ». Elle a d'ailleurs estimé que, s'il devait en être autrement, cela serait contraire à l'objectif même de la directive qui est d'assurer une « *protection efficace et complète des personnes concernées*[135] ».

---

[130] *Voy*. en ce sens C. KUNER, *European Data Protection Law. Corporate Compliance and Regulation, op.cit., p. 72*.
[131] *Voy. infra*.
[132] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, points 21 et s.
[133] Ibid., point 31.
[134] *Ibid*., point 33.
[135] *Ibid*., point 34.

Par sa décision, contraire à l'argumentation de l'Avocat général[136], la Cour a voulu permettre aux personnes concernées d'*effectivement* exercer leur droit à l'oubli. Certains auteurs critiquent d'ailleurs cet élargissement du champ d'application de la directive opéré par la Cour, considérant qu'un moteur de recherche n'a pas de contrôle sur les données publiées par les pages des sites internet qu'il référence[137]. De même, force est de constater que la position adoptée par le G29 dans son opinion de 2008 à l'égard des moteurs de recherche[138] était également plus nuancée, et identifiait « *plusieurs postures*[139] » ; seules certaines requéraient l'application de la directive[140].

Chapitre 3 : Quand, et pour quelle(s) raison(s) le droit à l'oubli peut-il être exercé ?

Section 1ère : Les principes généraux de qualité des données : un droit à l'oubli « passif »

§1er : Le principe de limitation de conservation des données

L'article 6, § 1er, e) prévoit que les données à caractère personnel doivent être conservées « *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* ». Malheureusement, aucune précision n'est donnée quant à la période maximale durant laquelle une donnée peut être conservée. Dans son opinion sur l'application des principes de nécessité et de

[136] *Voy*. les points 84 et s. des conclusions de l'Avocat général rendues sous l'arrêt *Google Spain*. Monsieur Jääskinen entendait notamment « *éviter la survenance de conséquences juridiques déraisonnables et excessives* » (conclusions, point 30).
[137] C. GAYREL, J. HERVEG et J.-M. VAN GYSEGHEM, « La protection des données à caractère personnel en droit européen », *J.E.D.H*., 2015, p. 77.
[138] Groupe de travail « Article 29 » sur la protection des données, « Opinion 1/2008 on data protection issues related to search engines », 4 avril 2008, 00737/EN WP 148.
[139] Formule employée par J. DUPONT-LASSALE, « Beaucoup de bruit pour rien ? La précarité du droit à l'oubli numérique consacré par la Cour de justice de l'Union européenne dans l'affaire Google Spain », *op.cit.*, p. 993.
[140] Le G29 avait en effet conclu à ce qui suit : « *Le principe de proportionnalité veut que, lorsqu'un fournisseur de moteur de recherche agit exclusivement en tant qu'intermédiaire, il ne soit pas considéré comme le principal responsable du traitement des données à caractère personnel effectué.* » *Voy*. Groupe de travail « Article 29 » sur la protection des données, « Opinion 1/2008 on data protection issues related to search engines », 4 avril 2008, 00737/EN WP 148, p. 15.

proportionnalité rendu en janvier 2014[141], le groupe de travail « Article 29 » précise néanmoins que les données doivent être stockées pour une période aussi courte que possible, faisant un parallèle avec le principe de « minimisation des données[142]. A cet égard, il renvoie à un arrêt rendu le 4 décembre 2008 par la Cour européenne des droits de l'homme, laquelle a jugé qu'une durée de conservation des données excessive ne pouvait satisfaire à la condition de « nécessité » dans une société démocratique, et allait dès lors à l'encontre du droit au respect à la vie privée[143]. Il faut cependant constater que cet arrêt a été rendu en matière d'ingérence dans la conservation des empreintes génétiques en cas d'acquittement ou de classement sans suite de personnes soupçonnées d'avoir commis des infractions. La transposition par analogie des enseignements de la Cour dans cette affaire à l'interprétation de la directive 95/46 n'est donc, à notre sens, pas si évidente.

Notons également que le texte ne donne aucune indication quant au sort qui doit être réservé aux données une fois celles-ci arrivées à leur terme. L'effacement, ou du moins l'anonymisation[144], cependant, semble être la solution la plus logique afin de concrétiser la fixation d'un délai de conservation. C'est également l'avis du G29 qui le mentionne expressément dans un avis relatif à la publicité comportementale[145]. Il recommande à cet égard de supprimer ou d'anonymiser immédiatement les « cookies » une fois que leur conservation n'est plus nécessaire.

Comme le révèle l'analyse faite ci-dessus, les responsables de traitement disposent donc malgré tout d'une large marge d'appréciation pour évaluer le temps durant lequel la conservation des données sert leur intérêt légitime[146]. Selon certains auteurs, un réseau social tel que Facebook pourrait fort bien considérer qu'une durée illimitée est légitimée par les besoins et la finalité de ses activités[147]. En matière de moteurs de recherche cependant, le G29 estime que cette durée ne peut être supérieure à six mois, laissant le choix aux États

[141] Groupe de travail « Article 29 » sur la protection des données, « Opinion 01/2014 on the applicable of necessity and proportionality concepts and data protection within the law enforcement sector », 27 février 2014, 536/14/EN WP 211, p. 18.
[142] *Voy. infra.*
[143] Cour eur. D.H., arrêt S. et Marper c. Royaume-Uni du 4 décembre 2008, points 35 et s., http://echr.coe.int (19 juin 2016).
[144] C. MARKOU, « The Right to Be Forgotten : Ten Reasons Why It Should Be Forgotten », *in Reforming European Data protection Law* (sous la dir. de P. DE HERT, S. GUTWIRTH et R. LEENES), Dordrecht, 2015, p. 207 ; S.Y. ESAYAS, « The rôle of anonymisation and pseudonymisation under the EU data rules : beyond the all or nothing approach », *E.J.L.T*, 2015, p. 19.
[145] Groupe de travail « Article 29 » sur la protection des données, « Opinion 2/2010 on online behavioural advertising », 22 juin 2010, 00909/10/EN WP 171, p. 20.
[146] J. AUSLOOS, H. GRAUX et P. VALCKE, « The Right to be Forgotten in the Internet Era », *ICRI Working Paper Series*, 2012, n°11, p. 10.
[147] *Ibid.*, p. 10.

membres d'exiger une période plus courte encore[148]. Au-delà de six mois, les moteurs de recherche seraient dans l'obligation de démontrer de façon détaillée en quoi la conservation des données est nécessaire pour les besoins du service[149].

Dès lors, même s'il est vrai qu'au plus l'information remonte dans le temps, au plus les intérêts de l'individu devraient prévaloir sur les intérêts publics[150], ce droit à l'oubli « passif[151] », en pratique, ne peut être surestimé[152].

§2 : Le principe de finalité

L'article 6, §1er, b), quant à lui, met en lumière la finalité pour laquelle le traitement des données à caractère personnel est effectué. Il stipule que ces dernières doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités*[153] ». Le principe sous-jacent exige du responsable de traitement des données qu'il fournisse explicitement à la personne concernée, dès le début de la collecte des données, une raison précise et légitime justifiant l'opération[154]. Par la suite, il ne pourra les exploiter que *de manière compatible* avec la finalité initialement présentée.

La difficulté réside évidement dans la définition de ce qui est ou non compatible avec la finalité. Les disparités importantes d'interprétation au sein des États membres, liées à la transposition de cette disposition dans leurs droits nationaux, ont d'ailleurs été soulignées par

[148] Groupe de travail « Article 29 » sur la protection des données, « Opinion 1/2008 on data protection issues related to search engines », 4 avril 2008, 00737/EN WP 148, p. 19.
[149] *Ibid*., p. 19.
[150] R.H. WEBER, « The Right to Be Forgotten : More Than a Pandora's Box ? », *op. cit*., p. 121.
[151] Dans le sens où il n'est pas nécessaire de faire une démarche. Il s'agit d'une sorte de droit à l'oubli automatique.
[152] J. AUSLOOS, H. GRAUX et P. VALCKE, « The Right to be Forgotten in the Internet Era », *op. cit*., p. 10. *A contrario*, certains auteurs estiment que la balance d'intérêt devrait se focaliser sur la valeur des données plutôt que sur l'éventuel risque de blesser les personnes concernées. Ainsi, bien que reconnaissant la difficulté de trouver un juste équilibre, Meg Leta Ambrose suggère que la priorité doit être donnée à la conservation des données. Celles-ci reflèteraient l'histoire et ne pourraient être supprimées que dans les cas les plus graves. *Voy*. M.L. AMBROSE, « It's About Time : Privacy, Information Life Cycles, and the Right to be Forgotten », *Stanford Technology Law Review*, 2013, Vol. 16, n° 2, p. 372.
[153] Art. 6, § 1er, b) de la directive 95/46.
[154] L. COLONNA, « Data Mining and Its Paradoxical Relationship to the Purpose Limitation Principle », *in Reloading Data Protection – Multidisciplinary Insights and Contemporary Challenges* (sous la dir. de P. DE HERT, S. GUTWIRTH et R. LEENES), Dordrecht, 2014, p. 303.

la Commission[155]. En 2013, le G29 a présenté une note explicative reprenant chacun des termes et proposant une définition pour chacun de ceux-ci. Elle se base également sur des exemples devant permettre une meilleure compréhension des notions et une meilleure cohérence dans leur application en pratique au sein de l'Union[156]. Il souligne en outre qu'un traitement de données réalisé à des fins différentes de celles pour lesquelles il était initialement prévu, n'implique pas *de facto* que ce traitement doit être considéré comme *incompatible*[157]. L'examen du principe de finalité doit dès lors s'opérer par une approche au cas par cas.

En matière de publicité comportementale, le G29 donne l'exemple d'un publicitaire qui ferait partie d'un groupe de sociétés. Si ce groupe prodigue un certain nombre de services, le publicitaire ne pourrait pas utiliser les données collectées dans le cadre des services proposés par le groupe (à moins qu'il ne puisse justifier d'une manière ou d'une autre que le traitement qu'il effectue est compatible avec la finalité initiale)[158].

Derrière ce principe, le législateur européen a surtout cherché à s'assurer que les individus comprennent la finalité pour laquelle leurs données vont être traitées, la manière dont elles seront utilisées, et à qui elles seront transférées[159]. Ainsi, le principe de finalité doit permettre à chaque personne concernée de faire un choix éclairé et de percevoir les dangers lorsqu'elle décide de transférer ses données[160], quitte à refuser de les fournir.

L'effacement, le verrouillage, l'interdiction du traitement des données, etc., sont autant de moyens possibles afin de mettre en œuvre le principe en cas de *traitement incompatible* des données[161]. L'anonymisation des données peut également être envisagée[162].

Cependant, pour des raisons évidentes qui tiennent au fonctionnement même de l'internet, la mise en pratique de cette limitation de temps est rendue pratiquement impossible[163].

---

[155] EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws », 2002, p. 29. http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE (19 mars 2016), p. 9.
[156] Groupe de travail « Article 29 » sur la protection des données, « Opinion 03/2013 on purpose limitation », 2 avril 2013, 00569/13/EN WP 203, pp. 20 et s.
[157] *Ibid.*, p. 21.
[158] Groupe de travail « Article 29 » sur la protection des données, « Opinion 2/2010 on online behavioural advertising », 22 juin 2010, 00909/10/EN WP 171, p. 20.
[159] L. COLONNA, « Data Mining and Its Paradoxical Relationship to the Purpose Limitation Principle », *op. cit.*, p. 304.
[160] Cour eur. D.H., arrêt Peck c. Royaume-Uni du 28 janvier 2003, point 62, http://echr.coe.int (14 avril 2016).
[161] Groupe de travail « Article 29 » sur la protection des données, « Opinion 03/2013 on purpose limitation », 2 avril 2013, 00569/13/EN WP 203, p. 37.
[162] C. DE TERWANGNE, « Internet Privacy and the Right to Be Forgotten/Right to Oblivion », *op. cit.,* p. 114.

§3 : Les principes de proportionnalité et de minimisation des données

Les principes de proportionnalité et de minimisation des données se dégagent de l'article 6, §1er, c) de la directive, lequel dispose que les données à caractère personnel doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement* ».

Pour juger du caractère « *adéquat* » d'une donnée, il faudrait que celle-ci soit « *utile*, *adaptée* et *complète* » au regard des finalités pour lesquelles elle sera traitée (en se plaçant du point de vue de la personne concernée)[164]. De même, une donnée « *pertinente* » doit s'entendre d'une donnée « *significative* », « *importante* », pour la réalisation d'une finalité précise du traitement[165].

Quant au caractère « non-excessif » que doivent revêtir les données, base du principe de minimisation des données, il s'agit ici de s'assurer que le nombre de données nécessaires à l'accomplissement de la finalité pour laquelle elles ont été collectées soit réduit à son strict minimum[166]. Christopher Kuner[167] prend pour exemple la loi fédérale allemande en matière de protection des données qui mentionne expressément l'obligation de traiter les données en n'en utilisant le moins possible et en rendant celles-ci anonymes chaque fois que cela est possible[168]. Certains considèrent d'ailleurs que lorsque l'utilisation des données est décrite comme étant « *à toutes fins utiles* », il faudrait en conclure que les données sont « *excessives* »[169].

Ces trois caractéristiques combinées forment, ensemble, ce que la doctrine appelle « le principe de proportionnalité », dans le contexte particulier qu'est celui de la directive

---

[163] Nous reviendrons plus tard sur les difficultés liées à la mise en pratique du droit à l'oubli. *Voy*. M.L. AMBROSE et J. AUSLOOS, « The Right To Be Forgotten Across The Pond », *Journal of Information Policy*, 2013, Vol. 3, p. 7.
[164] D. DE BOT, *Verwerking van persoonsgegens*, Antwerpen, Kluwer, 2002, p. 14, spéc. n°162.
[165] E. J. KINDT, *Privacy and Data Protection Issues of Biometric Applications – A Comparative Legal Analysis*, Dordrecht, Heidelberg, New York, London, Springer, 2013, p. 421.
[166] Groupe de travail « Article 29 » sur la protection des données, « Opinion 01/2014 on the applicable of necessity and proportionality concepts and data protection within the law enforcement sector », 27 février 2014, 536/14/EN WP 211, p. 16.
[167] C. KUNER, *European Data Protection Law. Corporate Compliance and Regulation*, *op. cit*., p. 31.
[168] *Voy*. la Section 3a de la loi fédérale allemande sur la protection des données. Une traduction anglaise est disponible: http://www.gesetze-im-internet.de/englisch_bdsg/.
[169] B. DOCQUIR, *Le droit de la vie privée*, Bruxelles, De Boeck, Larcier, 2008, p. 133, spéc. n°269.

95/46/CE[170]. L'article 6, §1er, c), *in fine*, suggère que le principe de proportionnalité et de minimisation doit être analysé en lien étroit avec le principe de finalité, déjà étudié plus haut.

Section 2 : Les articles 12 et 14 de la directive 95/46 : un droit à l'oubli « actif »

§1er: Le droit à l'effacement, à la rectification ou au verrouillage des données

A côté des différents principes relatifs à la qualité des données qui, de par leur caractère très général, permettent déjà aux individus un certain contrôle sur l'utilisation qui est faite de leur données, l'article 12, b) consacre expressément un « droit à l'effacement ». Intitulé « droit d'accès[171] », il stipule que toute personne concernée doit avoir « le droit d'obtenir du responsable du traitement selon le cas, *la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la […] directive, notamment en raison du caractère incomplet ou inexact des données* ». Contrairement à sa forme « passive[172] », ce versant « actif » du droit à l'oubli exige de la personne concernée une certaine démarche[173], et se distingue dès lors de la mise en œuvre, en principe, « automatique » de ce droit, lorsque, comme vu précédemment, il résulte d'une contravention à l'un des principes généraux[174]. Il doit donc être considéré, en tant que tel, comme étant un droit subjectif accordé aux personnes concernées[175].

Si les termes de « rectification » et « d'effacement » semblent relativement clairs, la notion de « verrouillage des données » paraît, quant à elle, plus difficile à cerner[176]. Or, la directive n'apporte aucune précision à ce sujet. La doctrine italienne traduit cette formule comme étant

[170] D. DE BOT, *Verwerking van persoonsgegens*, *op. cit*., p. 125, spéc. n°165.
[171] Gabriela Zanfir souligne le caractère curieux de cette dénomination et l'explique par le fait que le droit à l'effacement ne peut être exercé qu'après que la personne concernée ait appris, en tentant d'accéder à ses données, que ces dernières sont inexactes. *Voy.* G. ZANFIR, « Tracing the Right to Be Forgotten in the Short History of Data Protection Law : The New Clothes of an Old Right », *op. cit*., p. 241.
[172] Laquelle est issue des principes généraux relatifs à la qualité des données. *Voy.* art. 6 de la directive 95/46.
[173] B. KAMPMARK, « To Find or be Forgotten : Global Tensions on the Right to Erasure and Internet Governance », *Journal of Global Faultlines*, 2015, Vol. 2, n° 2, pp. 1-18.
[174] Xavier Duncan L'Hoiry et Clive Norris nous livrent une analyse détaillée de ces différents droits tels qu'intégrés dans les législations nationales des États membres. *Voy*. X. DUNCAN L'HOIRY et C. NORRIS, « The honest data protection officier's guide to enable citizens to exercise their subject access rights : lessons from a ten-country European study », *International Data Privacy Law*, 2015, pp. 190-204.
[175] A. FORDE, « Implications of the Right To Be Forgotten », *Tulane Journal of Technology & Intellectual Property*, 2015, p. 104.
[176] P.A. BERNAL, « A Right to Delete ? », *E.J.L.T.*, 2011, Vol. 2, n°2, p. 7.

le droit de bloquer toute opération de traitement qui concerne une information précise et spécifique, si les garanties accordées par le régime de la protection des données (entendez les différents principes de qualité de l'information[177] et de légitimité de traitement[178]) n'ont pas été observées[179]. Cela n'empêche qu'à défaut d'être défini par la directive, il revient aux courts et tribunaux des Etats membres ainsi qu'aux autorités nationales de protection des données, de résoudre cette question et d'appliquer le droit national transposant la directive « à la lumière[180] » des dispositions européennes. A titre d'exemple, les lois allemande et irlandaise clarifient la notion et définissent le verrouillage comme un moyen impliquant de « *marquer* » une donnée d'une manière qui permette d'empêcher son traitement, ou de faire en sorte qu'il ne soit pas possible de traiter la donnée en vue des finalités pour lesquelles la donnée a été « *marquée* ». La loi italienne fait plutôt référence à la « *suspension temporaire du traitement* », tandis que la loi suédoise renvoie à l'idée de « *restreindre l'utilisation d'une donnée bloquée* », et plus spécialement « *limiter sa diffusion* »[181].

On regrettera également l'absence d'indications relatives au choix à opérer entre rectification, effacement, ou verrouillage. Est-il possible de choisir expressément l'une des trois formules ? Si oui, comment ? Si non, comment savoir laquelle des trois formules sera appliquée ? La doctrine est particulièrement silencieuse à ce sujet. La traduction anglaise de la directive peut néanmoins s'avérer utile sur ce point. En effet, l'article 12, b) débute par les termes « *as appropriate the rectification, erasure or blocking of data* », ce qui suggère que le responsable de traitement des données est tenu de prendre la mesure *la plus appropriée* afin de répondre à la demande de la personne concernée. En pratique, cela signifierait qu'en cas d'erreur ou d'inexactitude, la mesure appropriée serait la rectification de l'information. Dans tous les autres cas, c.-à-d. lorsque la donnée pointée du doigt n'est pas conforme aux principes énoncés par l'article 6 de la directive, l'information devrait être effacée. Cette interprétation

[177] Art. 6 de la directive 95/46.
[178] Art. 7 de la directive 95/46.
[179] M. VIOLA DE AZEVEDO CUNHA, *Market Integration Through Data Protection — An Analysis of the Insurance and Financial Industries in the EU*, Dordrecht, Heidelberg, New York, London, Springer, 2013, p. 30, et les références citées.
[180] Notons que cette formule souvent utilisée dans le monde juridique n'apporte pas énormément de précision et laisse le champ libre aux institutions nationales pour interpréter la directive à leur convenance.
[181] Pour une analyse comparative de la mise en œuvre de la directive dans les législations des différents États membres, *voy*. K. DOUWE, « EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws », 2002, p. 29. http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE (19 mars 2016).

proposée par Douwe Korff[182] nous apparaît être la plus logique. Ce dernier va d'ailleurs plus loin, et estime que, dans ce dernier cas, ni le responsable des données, ni les autorités de protection des données ou les courts et tribunaux nationaux, n'auraient le droit d'apprécier le moyen – rectification, effacement ou verrouillage – le plus approprié[183].

A nouveau, à défaut de précision dans la directive, il revient toutefois aux États membres de régler cette question dans leurs droits national respectif.

A. Le caractère incomplet ou inexact des données

La formulation empruntée par le législateur européen semble permettre d'exiger l'effacement de données sans devoir en justifier substantiellement la raison[184]. Cependant, le champ d'application de cette prérogative se cantonne aux situations dans lesquelles le traitement des données viole les termes de la directive. A cet égard, l'article 12, b) fait explicitement référence au caractère « incomplet ou inexact » des données[185]. Se pose dès lors la question de savoir s'il est possible de demander l'effacement de données qui seraient complètes et exactes mais qui, en raison de leur caractère potentiellement nuisible pour la personne concernée, auraient tout intérêt à être effacées.

B. Raisons tenant aux principes énoncés aux articles 6 et 7 de la directive

L'exemple le plus illustratif de cette situation est celui des réseaux sociaux, sur lesquels un grand nombre d'utilisateurs « postent » des informations les concernant (photos, vidéos, anecdotes, opinions, etc.). Lorsque l'information est « inexacte[186] », la personne concernée est, comme nous venons de le voir, légalement en droit de demander à ce que celle-ci soit supprimée. En revanche, que faire d'une photo dérangeante correctement identifiée et publiée par un tiers ? L'emploi de l'adverbe « *notamment* », interprété comme « non-limitatif »,

[182] D. KORFF, *Data Protection Laws in the European Union*, Federation of European Direct Marketing & Direct Marketing Association, 2005, p. 97.
[183] *Ibid*., p. 97.
[184] B.-J. KOOPS, « Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right To Be Forgotten in Big Data Practice », *op. cit*., p. 12.
[185] *Voy*. également l'art. 6, d), de la directive 95/46.
[186] Bert-Jaap Koops dans l'exemple d'une personne qui serait erronément « taguée » sur une photo publiée sur un réseau social. L'identification de la personne concernée étant incorrecte, cette dernière serait en droit de demander l'effacement de la donnée. *Voy*. B.-J. KOOPS, « Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right To Be Forgotten in Big Data Practice », *op. cit*., p. 13.

suggère que des raisons autres que celles tenant au « *caractère incomplet ou inexact des données* » peuvent également servir d'argument pour demander le droit à l'effacement[187].

Cette lecture favorable aux personnes concernées, bien qu'ayant déjà fait pratiquement l'unanimité au sein des États membres lors de la transposition de la directive dans leurs législations nationales respectives, fut consacrée au niveau européen par la Cour de justice de l'Union européenne en mai 2014[188]. En effet, la Cour interprète la finale de l'article 12, b) comme « *révélant un caractère exemplatif et non exhaustif*[189] ». Elle ajoute en substance que la non-conformité du traitement avec les autres conditions de licéité imposées par la directive est également « *susceptible d'ouvrir à la personne concernée le droit* [à la rectification, l'effacement ou le verrouillage de données personnelles][190] ». Ces « *autres conditions de licéité* » doivent s'entendre comme étant l'ensemble des principes relatifs à la qualité des données énoncés à l'article 6 de la directive (le respect dû à ceux-ci étant cumulatif), ainsi que le respect d'au moins un des principes relatifs à la légitimation des traitements de données énumérés à l'article 7 de la même directive[191]. Autrement dit, il est possible de justifier la demande d'effacement de données (dans notre cas, une photo publiée par un tiers) parce que leur traitement ne correspond pas à l'un des principes vus plus haut (principe de limitation de conservation des données, principe de limitation de la finalité, principe de minimisation), ou parce que le traitement n'est pas « loyal » ou « licite[192] », ou parce que le responsable du traitement n'est pas en mesure de justifier le traitement des données au regard d'au moins un des principes énoncés à l'article 7 (par exemple, que la personne concernée a « *indubitablement donné son consentement*[193] », ou que le traitement est « *nécessaire à l'exécution d'un contrat auquel la personne concernée est partie*[194] »).

En pratique, il revient à la personne concernée d'apporter la preuve que le traitement de ses données enfreint au moins un des principes ci-dessus. Or, la tâche n'est pas toujours aisée, spécialement lorsqu'il s'agit de prouver la contrariété du traitement avec l'un des principes

[187] *Ibid*., p. 13.
[188] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12.
[189] *Ibid*., point n° 70.
[190] *Ibid*., point n° 70.
[191] *Ibid*., point n° 71 ; C.J.C.E., 20 mai 2003 (Österreichischer Rundfunk e.a.), C-465/00, C-138/01 et C-139/01, point 65, http://www.curia.europa.eu (13 mars 2016).
[192] Art. 6, §1er, a) de la directive 95/46.
[193] Art. 7, a), de la directive 95/46.
[194] Art. 7, b), de la directive 95/46.

issus de l'article 6. En effet, comment prouver, par exemple, que la photo a été publiée de façon inadéquate, ou excessive au regard des finalités pour lesquelles elle a été collectée ?

On peut alors penser à l'article 7, a) (en considérant que les articles 7, b) à e) sont inopérants), lequel prescrit, *a contrario*, que les données à caractère personnel ne peuvent être traitées si elles n'ont pas été indubitablement données avec le consentement de la personne concernée (c'est effectivement le cas dans notre exemple de la photo publiée par un tiers). La Cour ajoute d'ailleurs à ce propos que « *le traitement […] doit être légitimé en vertu de [l'] article 7 pour toute la durée pendant laquelle il est effectué*[195] ». Ainsi, quand bien même un consentement indubitable aurait été donné, il eut également fallu qu'il l'eût été durant toute la durée du traitement.

Cela est toutefois sans compter sur l'article 7, f) et la possibilité offerte au responsable de traitement des données de prouver que le traitement est « *nécessaire à la réalisation de l'intérêt légitime* » qu'il poursuit, ou que poursuivent le(s) tiers à qui les données ont été communiquées[196], « *à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, paragraphe 1er* ». Ainsi, dans notre exemple, même si le responsable de traitement arrive à prouver que la conservation de la photo est nécessaire à la réalisation de son intérêt légitime (en considérant bien sûr que la personne concernée n'est pas parvenue à prouver la contrariété du traitement avec l'un des principes de l'article 6), il sera encore possible de demander l'effacement des données, conformément à l'article 12, b). Tout l'enjeu est alors la balance des intérêts en présence : d'une part celui de la personne concernée et le respect de ses droits et libertés fondamentaux, en particulier le droit à la vie privée et à la protection de ses données personnelles, et, d'autre part, l'intérêt économique du responsable de traitement et/ou la liberté d'expression des internautes. Nous aborderons ce point plus longuement dans le chapitre suivant.

C. L'obligation de notification aux tiers.

Afin de rendre effectif les rectifications, l'effacement ou le verrouillage des données, l'article 12, c), instaure une obligation dans le chef des responsables de leur traitement de notifier aux

[195] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 95, *in fine*.
[196] En effet, comme vu précédemment, le responsable de traitement n'est pas tenu de satisfaire à l'ensemble des principes contenus à l'article 7. Seul un principe suffit.

tiers par lesquels ces données ont pu transiter et à qui elles ont pu être transmises des éventuelles modifications à effectuer. Cette obligation de notification connaît cependant deux limites. En effet, elle ne doit être respectée que dans la mesure où la tâche n'est pas impossible ou qu'elle « *ne suppose pas un effort disproportionné*[197] ». A cet égard, la doctrine a estimé que ces deux exceptions ne pouvaient être invoquées dans des situations purement internes. En revanche, subsiste la question de savoir si le responsable du traitement des données peut tout à fait méconnaître cette obligation lorsqu'il est en droit d'invoquer l'une des deux exceptions, ou s'il doit, malgré tout, faire son possible pour notifier aux tiers potentiels de ce que des données ont fait l'objet d'une correction[198].

§2 : Le droit d'opposition.

Le principe contenu dans le droit d'opposition provient initialement de l'idée que les individus *possèdent* leurs propres données et qu'ils devraient dès lors être en mesure de s'opposer à leur traitement. Il s'agirait de la « *reconnaissance évidente du droit à l'auto-détermination*[199] ».

Dans un rapport commentant le droit à l'oubli numérique récemment instauré par l'article 17 du nouveau règlement relatif à la protection des données, ce dernier est décrit comme « *la traduction lyrique du droit d'opposition dont dispose d'ores et déjà chaque personne dont les données ont été collectées*[200] ». En effet, comme mentionné précédemment, l'article 14 de la directive 95/46 octroie aux personnes concernées un droit général d'opposition au traitement de leurs données personnelles. D'après Anna Bunn, le droit d'opposition ne garantirait d'ailleurs aucune prérogative qui ne soit déjà accordée par l'article 12, b), mais « *oblige simplement le responsable de traitement ou l'autorité nationale à prendre plus spécifiquement en compte la situation de la personne concernée lorsqu'ils se prononcent sur*

[197] Art. 12, c), *in fine*.
[198] G. ZANFIR, « Tracing the Right to Be Forgotten in the Short History of Data Protection Law : The New Clothes of an Old Right », p. 243.
[199] J. DUMORTIER, E. KOSTA, A. KUCZERAWY et R. LEENES, « Regulating Identity Management », *in Digital Privacy. PRIME — Privacy and Identity Management for Europe* (sous la dir. de J. GAMENISH, R. LEENES et D. SOMMER), Berlin, Heidelberg, Springer, 2011, p. 84.
[200] CYBERLEX (L'association du droit et des nouvelles technologies), « Contribution dans le cadre des travaux sur el 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/wp-content/uploads/2015/10/contribution_cyberlex_dao.pdf (13 avril 2016). D'autres cependant contestent cette vision trop réductrice du droit d'opposition. *Voy*. C. BARTOLINI et L. SIRY, « The right to be forgotten in the light of the consent of the data subject », *Computer Law & Security Review*, 2016, p. 225.

la légitimité du traitement basée sur les articles 7, e), ou 7, f)[201] ». C'est également l'interprétation que la Cour semble avoir donnée à l'article 14 dans le cadre de son arrêt *Google Spain*[202]. La loi grecque transposant la directive confond d'ailleurs le droit d'opposition et les droits reconnus au titre de l'article 12, b)[203]. Cependant, faisant partie intégrante du régime juridique du droit à l'oubli, il nous semble important de présenter ses principales caractéristiques et d'en définir les contours.

L'article 14, a), oblige les États membres à accorder le droit aux personnes concernées de s'opposer « *à tout moment, pour des raisons prépondérantes et légitimes tenant à* [leur] *situation particulière, à ce que des données* [les] *concernant fassent l'objet d'un traitement* ». Le champ d'application de cette disposition reste néanmoins limité[204] et ne trouve à s'appliquer que lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public[205] ou lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement[206]. De plus, le droit national est autorisé à restreindre la portée donnée au droit d'opposition[207]. Les États membres ne sont donc pas tenus de créer un droit d'opposition lorsque les personnes concernées ont donné leur plein accord préalablement au traitement de leur données dans les cas visés aux articles 7, a), b), c) et d) (traitement nécessaire à l'exécution d'un contrat, au respect d'une obligation légale ou à la sauvegarde de l'intérêt vital de la personne concernée) [208].

La personne concernée sera tenue de prouver le caractère illégitime de la poursuite du traitement, mais également que son intérêt propre est supérieur à celui de l'intérêt public ou

---

[201] A. BUNN, « The curious case of the right to be forgotten », *Computer Law & Security Review*, 2015, pp. 343-344.

[202] La Cour s'exprime en ces termes : « *La pondération à effectuer dans le cadre dudit article 14, premier alinéa, sous a), permet ainsi de tenir compte de manière plus spécifique de toutes les circonstances entourant la situation concrète de la personne concernée. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable de celui-ci ne peut plus porter sur ces données*. » *Voy*., C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 76.

[203] K. DOUWE, « EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws », *op. cit*., p. 112. Douwe Korff, EC study on implementation of data protection directive, p. 112. *Voy*. également C. BARTOLINI et L. SIRY, « The right to be forgotten in the light of the consent of the data subject », *op. cit*., p. 224, spéc. point 3.2.

[204] Le considérant n°25 de la directive 95/46 parle de « *certaines circonstances* ».

[205] Art. 7, e), de la directive 95/46.

[206] Art. 7, f), de la directive 95/46.

[207] Art. 14, a), de la directive 95/46. *Voy*. C. BARTOLINI et L. SIRY, « The right to be forgotten in the light of the consent of the data subject », *op. cit*., p. 224.

[208] J. AUSLOOS, « The Right to be Forgotten — Worth Remembering ? », *Computer Law & Security Review*, 2012, p. 150.

du responsable de traitement[209]. De surcroît, il n'est possible de s'opposer au traitement des données que pour le futur. En d'autres termes, le responsable de traitement ne sera pas tenu de *supprimer* les données ayant déjà été traitées. L'obligation ne porte que sur le traitement futur de ces données[210].

En pratique, la personne concernée pourra tout d'abord adresser ses demandes au responsable de traitement, lequel « *doit alors dûment examiner le bien-fondé de celles-ci et, le cas échéant, mettre fin au traitement des données en cause*[211] ». Si le responsable de traitement répond par la négative, l'affaire peut être portée devant l'autorité nationale de protection des données ou devant une autorité judiciaire « *pour que celles-ci effectuent les vérifications nécessaires et ordonnent à ce responsable des mesures précises en conséquence*[212] ».

Afin de permettre aux autorités nationales d'évaluer au mieux les demandes formulées par les personnes concernées, le G29 a publié des lignes de conduite[213] contenant une liste de critères communs à prendre en compte[214]. La liste n'est pas exhaustive. Les critères mentionnés ne sont pas cumulatifs et doivent être lus dans le respect de la législation nationale, permettant certaines variantes d'interprétation d'un État membre à l'autre[215].

Enfin, relevons que l'article 14, b), permet de s'opposer gratuitement au traitement de données lorsque celui-ci est effectué à des fins de prospection (entendez marketing direct).

---

[209] D. GEORGE et A. TAMO, « Ein Europäisches Recht auf Vergessen – eine Schweizer Pflicht zum Löschen? — Thesen zum möglichen Einfluss von Art. 17 des DSG-VO Entwurfes auf multinationale Unternehmen in der Schweiz », *in Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft* (sous la dir. de S. BRÄNDLI, R. SCHISTER et A. TAMO), Bern, 2013, p.49.

[210] Il n'est dès lors pas possible, sur base de la directive actuelle, de demander la suppression de données purement et simplement parce que l'on retire son consentement. Le retrait du consentement n'affecte que le traitement futur des données. *Voy*. Groupe de travail « Article 29 » sur la protection des données, « Opinion 15/2011 on the definition of consent », 13 juillet 2011, 01197/11/EN WP 187.

[211] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 77. Notons que la Cour n'explique pas ce que veut dire « *mettre fin au traitement* ». Cela implique-t-il l'effacement, ou le verrouillage des données ? Nous optons pour une solution appropriée, en fonction du cas d'espèce.

[212] *Ibid*., point 77.

[213] Groupe de travail « Article 29 » sur la protection des données, « Guidelines on the implementation of the Court of Justice of the European Union judgement on Google Span and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González C-131/12 », 26 novembre 2014, 14/EN WP 225, pp. 13 et s.

[214] Cette liste de critères est initialement prévue afin de répondre aux demandes de déréférencement mais devrait également pouvoir s'appliquer dans le cadre de demandes d'effacement de manière générale. *Voy*. C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit*., p. 266 ; G. ZANFIR, « How CJEU's Privacy Spring constructed the human rights shield in the digital age », 2015, p. 10, http://www.academia.edu/12458989/How_CJEU_s_Privacy_Spring_construed_the_human_rights_shield_in_the_digital_age (13 février 2016).

[215] Groupe de travail « Article 29 » sur la protection des données, « Guidelines on the implementation of the Court of Justice of the European Union judgement on Google Span and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González C-131/12 », 26 novembre 2014, 14/EN WP 225, p. 12.

Dans ce cas, il n'est plus nécessaire de justifier d'un intérêt particulier. Les Etats membres ont alors le choix entre deux formules : soit donner le droit aux personnes concernées de s'opposer directement au traitement de leurs données à des fins de prospection, soit leur donner le droit d'être préalablement informés avant que leurs données ne soient transmises à des tiers pour être exploitées à des fins de prospection. La procédure et les délais à observer pour bénéficier d'un tel droit doivent être réglés par les Etats membres[216].

Chapitre 4 : Balance des intérêts entre le droit à la protection des données personnelles et le droit à la liberté d'expression

Très souvent cité dans la doctrine pour la force de ses propos, Jeffrey Rosen assurait en 2012 que le droit à l'oubli « *represents the biggest threat to free speech on the Internet in the coming decade*[217] ». Sa déclaration intervenait peu de temps après que Viviane Reding, alors Commissaire européenne à la justice, aux droits fondamentaux et à la citoyenneté, annonçait[218] la création d'un nouveau droit à l'oubli numérique dans la proposition de règlement de la Commission européenne. Des réactions similaires[219], principalement en provenance des États-Unis, ont par la suite envahient le débat lié au droit à l'oubli numérique lorsque la Cour de justice de l'Union européenne[220] s'est officiellement positionnée en faveur de la protection des données personnelles face aux intérêts des internautes et de l'exploitant d'un moteur de recherche[221].

---

[216] A. FAIRCHILD, E. KOSTA, R. LEENES et B. PRIEM, « The Need for Privacy-Enhancing Identity Management », *in Digital Privacy. PRIME – Privacy and Identity Management for Europe* (sous la dir. de J. GAMENISH, R. LEENES et D. SOMMER), Berlin, Heidelberg, Springer, 2011, p. 62.

[217] J. ROSEN, « Symposium Issue. The Right To Be Forgotten », *Stanford Law Review Online*, Vol. 64, 2012, p. 88 : « *Le droit à l'oubli représente la plus grande menace à la liberté d'expression sur internet pour les décennies à venir.* »

[218] V. REDING, « Privacy matters – Why the EU needs new personal data protection rules », SPEECH/10/700, discours prononcé à Bruxelles le 30 novembre 2010 dans le cadre de la *European Data Protection and Privacy Conference*.

[219] M. FORD, « Will Europe Censor This Article? », The Atlantic, 13 mai 2014, http://www.theatlantic.com/international/archive/2014/05/europes-troubling-new-right-to-be-forgotten/370796/ (14 novembre 2015).

[220] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12.

[221] Ce n'est toutefois pas le cas de tous. Certains saluent la décision de la Cour et reconnaissent la nécessité de limiter à certains égards la liberté d'expression lorsque celle-ci empêchent la reconstruction de la réputation mise à mal par des erreurs passées. *Voy*. à ce propos J., ABRAMSON, « Searching for Reputation : Reconciling

Afin de mieux comprendre les intérêts en jeux et la position de la Cour, nous analyserons successivement ces deux libertés et les facteurs dont il faut tenir compte lors de la mise en balance des droits des différentes parties en présence.

Section 1ère : Le cadre prévu par le droit de l'Union

Lorsque les données litigieuses sont diffusées par un tiers, les droits de ce dernier, tel que sa liberté d'expression, se heurtent bien souvent au droit à la protection des données personnelles[222] et à la vie privée[223] de la personne concernée[224]. Les journalistes, par exemple, utilisent de plus en plus souvent les tweets ou commentaires laissés par des internautes pour agrémenter leurs articles d'opinions divers, facilement accessibles sur Internet[225]. Le conflit qui peut en résulter donne alors lieu à un exercice délicat de mise en balance des différents droits fondamentaux en présence[226]. A cet égard, la Cour de justice de l'Union européenne laisse bien souvent le soin aux États membres d'adopter les mesures nécessaires afin de garantir leur protection[227].

Dans l'affaire *Google Spain*, c'est le droit à l'information, composante du droit à la liberté d'expression protégée par l'article 11 de la Charte des droits fondamentaux, et le droit à la liberté d'expression et la liberté d'entreprendre[228] de Google qui était en jeu. La Cour a tranché elle-même la question de cet équilibre et a jugé que les droits de la personne concernée « *prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche mais également sur l'intérêt* [du] *public* » qui souhaiterait trouver des informations relatives à la personne concernée « *lors d'une recherche portant sur le nom de*

Free Speech and the Right To Be Forgotten », *North Carolina Journal of Law & Technology*, 2015, Vol. 17, n° 1, p. 71.

[222] Art. 8 de la Charte des droits fondamentaux de l'Union européenne, C 364, *J.O.C.E.*, 18 décembre 2000, p. 1

[223] *Ibid*., art. 7.

[224] M. HOVEN, « Balancing Privacy and Speech in the Right to Be Forgotten », *Harvard Journal of Law & Technology*, 2012, http://jolt.law.harvard.edu/digest/privacy/balancing-privacy-and-speech-in-the-right-to-be-forgotten (18 octobre 2015), p. 9.

[225] R.L. BOLTON, « The Right To Be Forgotten : Forced Amnesia in a Technological Age », *Journal of Information Technology & Privacy Law*, 2014, Vol. 31, p. 141.

[226] M. FAZLIOGLU, « Forget me not : the clash of the right to be forgotten and freedom of expression on the Internet », *International Data Privacy Law*, 2013, p. 150 ; M. BASSINI et O. POLLICINO, « Reconciling the right to be forgotten and freedom of information in the digital age. Past and future of personal data protection in the EU », 2013, http://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wccl-cmdc/wccl/papers/ws14/w14-Pollicino&Bassini.pdf (12 octobre 2014).

[227] *Voy*. J. DUPONT-LASSALE, « Beaucoup de bruit pour rien ? La précarité du droit à l'oubli numérique consacré par la Cour de justice de l'Union européenne dans l'affaire Google Spain », *op. cit*., p. 1008 et les références citées.

[228] Art. 16 de la Charte des droits fondamentaux de l'Union européenne.

cette personne[229] ». Cette décision surprend[230] tant elle est opposée aux conclusions de l'Avocat général Jääskinen qui avait préconisé la solution inverse[231]. Cependant, l'exercice d'équilibriste effectué par la Cour se cantonne à l'affaire en cause et on ne pourrait en déduire qu'une solution identique trouverait à s'appliquer chaque fois qu'un internaute fait usage de son « droit à l'oubli ». Elle rappelle d'ailleurs « *que cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment en fonction du rôle joué par cette personne dans la vie publique*[232] ». En ce sens, la Cour avait également jugé en 2006 « *qu'il appartient aux autorités et aux juridictions nationales chargées d'appliquer la réglementation nationale transposant la directive 95/46 d'assurer un juste équilibre des droits et intérêts en cause, y compris les droits fondamentaux protégés par l'ordre juridique communautaire*[233] », cet équilibre devant être proportionné et devant tenir compte des circonstances de l'espèce[234].

A cet égard, le fait que le responsable de traitement soit un moteur de recherche, lequel permet aisément de rassembler un grand nombre d'informations relatives à la personne concernée « *et peut jouer un rôle décisif pour la diffusion desdites informations*[235] », constitue, d'après la Cour, un élément essentiel lors de la mise en balance des intérêts. Au contraire des sites *Web*, lesquels n'offrent bien souvent que des informations éparses, pouvant sembler insignifiantes, un moteur de recherche permet quant à lui de reconstituer un « profil »

[229] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 97.
[230] Pour un inventaire des réactions des différents acteurs concernés (tels que les grandes entreprises de l'internet), *voy*. I. SPAHIU, « Between the right to know and the right to forget : looking beyond the Google case », *E.J.L.T.*, 2015, Vol. 6, n° 2, pp. 5-7.
[231] Celui-ci s'était exprimé en ces termes : « *Je dissuaderais également la Cour de conclure que ces intérêts concurrents pourraient être mis en balance de façon satisfaisante dans les situations individuelles, sur la base d'une analyse au cas par cas, en laissant aux fournisseurs de services de moteur de recherche sur Internet le soin de statuer. De telles «procédures de notification et de retrait», si elles étaient exigées par la Cour, conduiraient vraisemblablement soit au retrait automatique de liens vers tout contenu faisant l'objet d'une opposition, soit à un nombre ingérable de demandes traitées par les fournisseurs de services de moteur de recherche sur Internet les plus populaires et importants*. » *Voy*. point 133 des conclusions de l'Avocat général sous l'arrêt *Google Spain*.
[232] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 81.
[233] C.J.C.E., 6 novembre 2003 (Bodil Lindqvist), C-101/01, point 90.
[234] *Ibid.,* point 88.
[235] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, point 87.

de la personne concernée via des données agrégées[236] et ainsi rendre n'importe quelle personne clairement identifiable[237].

La notion « d'intérêt public » se présente, elle aussi, comme un critère important dont il faut tenir compte dans le processus de mise en balance des intérêts[238]. Il s'agit d'une exception au droit à l'oubli, ou, *in casu*, au droit au déréférencement, fort critiquée par la doctrine[239]. Ainsi, s'il apparaît que l'ingérence dans les droits fondamentaux de la personne concernée est justifiée par l'intérêt du public à avoir accès aux informations faisant l'objet du litige, la personne concernée perdra son droit d'obtenir l'effacement, ou à tout le moins le déréférencement de ses données. Quant à la question de savoir ce qui est « d'intérêt public », la question reste relativement floue et relève de l'appréciation effectuée par le responsable de traitement. Faut-il conclure que des informations liées au passé d'une figure publique, publiées avant que celle-ci ne devienne connue, puissent être qualifiées de privées[240] ? Cette question est soumise à controverse, bien que l'on puisse légitimement argumenter en faveur d'un droit à l'oubli du lointain passé. Menteur ou exceptionnellement sage serait celui qui n'aurait pas le moindre remord vis-à-vis d'une ou l'autre de ses actions passées[241]. Les critiques pointent également du doigt, avec raison selon nous, les efforts, les coûts et le temps perdu[242] que les responsables de traitement devront désormais consacrer à cette tâche en devenant des « censeurs [243] ».

La question de l'adéquation, de la pertinence ou du caractère non-excessif des données au regard des finalités pour lesquelles elles ont été collectées est bien entendu un critère à prendre en compte.

---

[236] I. SPAHIU, « Between the right to know and the right to forget : looking beyond the Google case », *op. cit*., p. 8.
[237] C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, points 36 et 80.
[238] *Ibid*., point 97, *in fine*.
[239] I. SPAHIU, « Between the right to know and the right to forget : looking beyond the Google case », *op. cit*., p. 9.
[240] J. WAKEFIELD, « Politician and paedophile ask Google to be forgotten », BBC NEWS, 15 mai 2014, http://www.bbc.com/news/technology-27423527 (17 juin 2016).
[241] I. SPAHIU, « Between the right to know and the right to forget : looking beyond the Google case », *op. cit*., p. 10.
[242] Emily Shoor soulève par exemple qu'il pourrait être nécessaire d'engager de nouveaux employés pour répondre aux demandes. *Voy*. E.A SHOOR., « Narrowing the Right to be Forgotten : Why the European Union needs to amend the Proposed Data Protection Regulation », op. cit., p. 505.
[243] *Ibid*., p. 488.

Afin de palier en partie aux difficultés liées à la mise en œuvre des différents éléments soulignés par la Cour, le G29 a publié des lignes directrices[244] établissant une liste de treize critères à prendre en compte lors du traitement des plaintes[245] :

1. Les résultats de recherche sont-ils liés au nom ou au pseudonyme d'une personne physique permettant facilement de l'identifier ?
2. La personne concernée joue-t-elle un rôle dans la vie publique ? S'agit-il d'une figure publique[246] ?
3. La personne concernée est-elle mineure ?
4. Les données sont-elles erronées ?
5. Les données sont-elles pertinentes et non-excessives[247] ? Sont-elles liées à la profession de la personne concernée ? Les résultats de la recherche mènent-ils à des informations pouvant être interprétées comme des discours de haine, à de la calomnie ou de la diffamation ou tout autre préjudice du même type à l'encontre de la personne concernée ?
6. L'information est-elle « sensible » au sens de l'article 8 de la directive 95/46/CE[248] ?
7. Les données sont-elles à jour ? Ont-elles été disponibles pour une période supérieure à celle nécessaire à la réalisation des objectifs pour lesquels elles ont été traitées ?
8. Le traitement de ces données a-t-il causé un préjudice à la personne concernée ? Et si oui, est-il disproportionné ?
9. Les données mènent-elles vers des informations susceptibles de placer la personne concernée en danger ?
10. Dans quel contexte l'information a-t-elle été publiée ? Le contenu a-t-il été volontairement rendu public ? La personne concernée pouvait-elle raisonnablement s'attendre à ce que le contenu soit rendu public ?
11. Le contenu original de ces données a-t-il été publié à des fins journalistiques ?
12. L'éditeur des données a-t-il un droit ou une obligation légale de rendre ces données publiques ?

[244] Groupe de travail « Article 29 » sur la protection des données, « Guidelines on the implementation of the Court of Justice of the European Union judgement on Google Span and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González C-131/12 », 26 novembre 2014, 14/EN WP 225.
[245] Traduits ou résumés par nous.
[246] Les hommes politiques, les hommes d'affaires, ou les professions réglementées telles que la profession d'avocat ou de médecin sont donnés à titre d'illustration.
[247] Cette question relève du principe de proportionnalité vu plus haut. *Voy. supra.*
[248] Ces données sont alors liées à l'origine raciale ou ethnique, ou révèlent des opinions politiques, des convictions religieuses, etc.

13. Les données sont-elles liées à une infraction pénale ?

Dans l'ensemble, chacun de ces critères est lié à la pertinence des informations diffusées.

Nous soulignerons enfin que la jurisprudence de la Cour a permis par le passé de traiter la question sous une autre forme. Dans un second arrêt *Satamedia*[249], le problème fut attaqué sous l'angle de l'article 9 de la directive 95/46 et de l'exception « *aux seules fins journalistiques* »[250]. En effet, l'article 9 permet aux États membres de prévoir, « *pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations* [au droit à la protection des données] *dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression* ». Ainsi, plutôt que d'affronter les difficultés liées à la mise en balance de droits fondamentaux entre eux, la question portait sur la notion de « *fins journalistiques* » et sa signification dans le droit de l'Union[251]. La Cour avait alors opté pour une interprétation large du concept tout en précisant que des limitations au droit à la protection des données ne seraient tolérées que pour autant qu'elles soient « *strictement nécessaires*[252] ». Elles avaient présenté les « activités de journalisme » au sens de l'article 9 de la directive comme « [ayant] *pour finalité la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que ce soit*[253] ». Cette définition permet ainsi de couvrir non seulement les entreprises de médias mais également les particuliers lorsqu'ils procèdent à ce type d'activité.

La plus haute juridiction administrative finlandaise, chargée en dernier ressort de l'affaire en cause au niveau national, avait également jugé, sur base des conclusions de l'Avocat général Kokott, qu'il fallait, en outre, tenir compte de la mesure dans laquelle l'ingérence dans les

[249] C.J.U.E., 16 décembre 2008 (*Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*), C-73/07, http://www.curia.europa.eu (14 juin 2016). Le premier étant l'arrêt *Lindqvist* et le troisième *Google Spain* (arrêts dans lesquels la Cour met en balance la protection des données avec la liberté d'expression).
[250] *Voy*. également le considérant 37 de la directive 95/46. En substance, cet angle d'approche correspond au 11e critère énoncé par le G29 dans ses lignes directrices relatives à la mise en œuvre de l'arrêt *Google Spain*.
[251] Pour une analyse approfondie de la notion de « *fins journalistiques* », *voy*. D. ERDOS, « Confused ? Analysing the Scope of Freedom of Speech Protection vis-à-vis European Data Protection », University of Oxford Legal Research Paper Series, Paper n° 48/2012, 2012, pp. 1-36, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2119187 (17 mars 2016).
[252] C.J.U.E., 16 décembre 2008 (*Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*), C-73/07, point 56. A ce propos, *voy*. le commentaire de C. BAGGER TRANBERG, « Proportionality and data protection in the case law of the European Court of Justice », *International Data Privacy Law*, 2011, p. 244.
[253] *Ibid*., point 61.

droits fondamentaux de la personne concernée pouvait contribuer au débat public[254]. Elle avait alors jugé que dans le cas d'espèce, l'information n'avait pas été diffusée afin de contribuer à l'intérêt d'un débat social mais ne faisait que servir la curiosité de quelques individus privés[255]. Cette solution pourrait, selon nous, permettre d'appuyer une argumentation basée uniquement sur la balance entre les droits fondamentaux.

Section 2 : Le cadre prévu par la Convention européenne des droits de l'homme

Bien qu'appartenant à un ordre juridique distinct, la Convention européenne des droits de l'homme (CEDH)[256] est également un instrument juridique de taille, fort utile aux juridictions européennes. En effet, si l'Union européenne n'est pas signataire de la Convention[257], ce n'est pas le cas des États membres qui l'ont, quant à eux, tous signée[258]. La Cour de justice de l'Union a d'ailleurs mainte fois expressément reconnu la nécessité, dans le chef des Cours et tribunaux nationaux, de tenir compte de la jurisprudence de la Cour de Strasbourg lorsqu'ils sont amenés à interpréter des dispositions instituant des droits fondamentaux[259]. Il est donc possible d'en conclure que tant la jurisprudence de Strasbourg que celle de Luxembourg sont pertinentes en matière de droits fondamentaux[260].

Or, il se trouve que l'article 10 de la CEDH reconnaît également le droit à la liberté d'expression. Face à cette disposition, l'article 8 de la CEDH protège quant à lui la vie

[254] D. ERDOS, « Confused ? Analysing the Scope of Freedom of Speech Protection vis-à-vis European Data Protection », *op. cit.,* pp. 15-16 ; C.E. CARBONE, « To Be or Not To Be Forgotten : Balancing the Right to Know with the Right to Privacy in the Digital Age », *Virginia Journal of Social Policy & the Law*, 2015, Vol. 22, n° 3, p. 542.
[255] *Voy*. J. AUSLOOS , A. KUCZERAWY et B. VAN ALSENOY, « Search engines after Google Spain : internet@liberty or privacy@peril? », KU Leuven ICRI Working Paper Series n° 15/2013, 2013, p. 57, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494 (17 février 2015).
[256] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950.
[257] *Voy*. l'avis de la Cour à ce sujet : Avis 2/13 de la Cour (assemblée pléniaire) du 18 décembre 2014 rendu en vertu de l'article 218, paragraphe 11, TFUE, relatif à l'adhésion de l'Union européenne à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.
[258] Pour la liste complète des États signataire, *voy*. www.coe.int.
[259] *Voy*. J. KOKOTT et C. SOBOTTA, « The Charter of Fundamental Rights of the European Union After Lisbon », EUI Working Paper AEL, European University Institute, 2010, n° 6, p. 2, et les références citées.
[260] O. DE SCHUTTER et F. TULKENS, « Rights in Conflict : the European Court of Human Rights as a Pragmatic Institution », *in Conflicts Between Fundamental Rights* (sous la dir. de E. BREMS), Antwerpen, Oxford, Portland, Intersentia, 2008, p. 182.

privée, ce qui comprend, entre autre, le droit à la protection des données personnelles[261]. Dans les deux cas, il s'agit de droits « non-absolus » dans le sens où tous deux peuvent être soumis à des restrictions et être mis en balance avec d'autres droits fondamentaux[262]. Dès lors, à l'instar de la Charte des droits fondamentaux de l'Union européenne, la CEDH n'établit aucune prévalence d'un droit fondamental vis-à-vis d'un autre. Une balance d'intérêt doit, ici aussi, être opérée au cas par cas. Les enseignements de la Cour de Strasbourg sont donc tout à fait pertinents à cet égard[263].

Ainsi, dans un arrêt *Aleksey Ovchinnikov*[264], la Cour a jugé que « *dans certains cas, il peut être justifié de limiter la reproduction d'informations déjà entrées dans le domaine public, par exemple pour empêcher que continuent d'être diffusés les détails de la vie privée d'une personne hors de tout débat politique ou public portant sur un sujet d'intérêt général*[265] ».

L'un des critères fondamentaux employé par la Cour est ainsi de savoir si la liberté d'expression en cause contribue d'une manière ou d'une autre à un débat d'intérêt général[266].

De même, la question de la manière dont l'information en cause a été obtenue revêt une importance toute particulière[267]. La Cour tient également compte de la nature même d'Internet, permettant à des milliers de personnes à travers le monde d'avoir accès à des données et des informations sensibles. Elle considère donc que l'ingérence occasionnée au droit à la protection des données s'en retrouve nettement aggravée[268].

---

[261] Quant à la reconnaissance du droit à la protection des données comme faisant partie du droit à la vie privée, voy. notamment Cour eur. D.H., arrêt I. c. Finlande du 17 juillet 2008, http://echr.coe.int (19 juin 2016) ; Cour eur. D.H., arrêt K.U. c. Finlande du 2 décembre 2008, http://echr.coe.int (19 juin 2016) ; Cour eur. D.H., arrêt S. et Marper c. Royaume-Uni du 4 décembre 2008, spéc. point 103, http://echr.coe.int (19 juin 2016).

[262] L'art. 10, §2, de la Convention, précise par exemple très clairement que certaines restrictions doivent parfois être imposées afin de protéger « […] *la réputation ou des droits d'autrui* ».

[263] Pour un aperçu de la jurisprudence de la CEDH à l'égard de la protection des données personnelles, *voy*. la fiche thématique proposée par l'Unité de la Presse de la CEDH, disponible à l'adresse suivante : http://www.echr.coe.int/Documents/FS_Data_fra.pdf.

[264] Cet arrêt est cité à titre d'illustration par l'Avocat général Jääskinen dans ses conclusions relatives à l'affaire *Google Spain. Voy. cooncl*usion, *point 127.*

[265] Cour eur. D.H., arrêt Aleksey Ovchinnikov c. Russie du 16 décembre 2010, point 50, http://echr.coe.int (19 juin 2016).

[266] *Voy*. par exemple Cour eur. D.H., arrêt Von Hannover c. Allemagne du 7 février 2012, http://echr.coe.int (19 juin 2016).

[267] Cour eur. D.H., arrêt Axel Springer AG c. Allemagne du 7 février 2012, point 93, http://echr.coe.int (19 juin 2016). La Cour établit une liste de critères pertinents pour la mise en balance tels que la contribution à un débat d'intérêt général, la notoriété de la personne visée et l'objet des données, le comportement antérieur de la personne concernée, le mode d'obtention des informations et leur véracité, le contenu, la forme et les répercussions de la publication, la gravité de la sanction imposée, etc. (*voy*. points 89 et s.)

[268] Cour eur. D.H., arrêt Węgrzynowski et Smolczewski c. Poland du 16 juillet 2013, point 58, http://echr.coe.int (19 juin 2016).

Chapitre 5 : Le nouveau règlement général de protection des données

Depuis fin avril 2016, l'Union européenne s'est dotée d'un nouveau règlement en matière de protection des données personnelles[269]. Au cœur de cette réforme, la consécration du droit à l'oubli dans un texte européen fut la source des plus vives critiques de la part de ses détracteurs[270]. Certains ont tentés de proposer des alternatives à l'interprétation stricte et littérale du nouveau texte européen en conciliant les points de vue américain et européen[271]. Cependant, les défis que « *l'évolution technologique rapide et la mondialisation* » posaient à notre société, rendaient nécessaire la révision de la directive 95/46[272]. On ne peut donc que saluer l'initiative de la Commission[273].

Le droit à l'oubli, bien que présenté comme un « droit à l'effacement » à l'article 17 du nouveau règlement, est expressément mentionné dans ses considérants 65 et 66. Ce dernier serait particulièrement pertinent « *lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur internet*[274] ». Ces termes font échos à la présentation du droit à l'oubli réalisée par Viviane Reding lors de la Conférence européenne pour la protection des données et la vie privée tenue en janvier 2012 à Munich. Elle déclarait alors que dans le contexte numérique actuel, dans lequel un nombre croissant de données personnelles circulent sur le Web, spécialement sur les réseaux sociaux, les personnes devraient se voir octroyer le droit — et

[269] Règl. (UE) n° 2016/679 (*voy*. n° 2).
[270] D. JACOBS et M. ROTTENBERG, « Updating the Law of Information Privacy : The New Framework of the European Union », *Harvard Journal of Law & Public Policy*, 2013, Vol. 36, n° 2, p. 632 et les références citées.
[271] S.C. BENNETT, « The Right to Be Forgotten : Reconciling EU and US Perspectives », *Berkeley Journal of International Law*, 2012, Vol. 30, n° 1, pp. 161-195 ; P. BRUENING , S. CARTER et D. HOFFMAN, « The Right to Obscurity : How We Can Implement the Google Spain Decision », *North Carolina Journal of Law & Technology*, 2016, Vol. 17, n° 3, pp. 437-481 ; S. KULEVSKA et M.L. RUSTAD, « Reconceptualizing the Right To Be Forgotten To Enable Transatlantic Data Flow », *Harvard Journal of Law & Technology*, 2015, Vol. 28, n°2, pp. 349-417.
[272] La Commission a tout de même souligné que les principes fondamentaux de la directive étaient toujours d'actualité. *Voy*. 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 donnés à caractère personnel dans l'Union européenne », *C.O.M.* (2010) 609 final.
[273] P. BLUME, « The myths pertaining to the proposed General Data Protection Regulation », *International Data Privacy law*, 2014, p. 273.
[274] Considérant 65 du règlement 2016/679.

non pas la possibilité[275] — de faire entièrement supprimer leurs données[276]. Ainsi, cette nouvelle version du droit à l'oubli semble avant tout cibler des données librement diffusées par la personne concernée qui, par la suite, aurait des remords à voir ces informations indéfiniment[277] conservées sur la toile[278]. Cependant, il devrait également permettre de demander la suppression de données automatiquement collectées, tels que les adresses IP ou les cookies[279], grâce à la définition large de la nouvelle notion de « données à caractère personnel[280] ».

Dans le cadre de cette étude, nous commencerons par dresser un portrait détaillé du contenu et du champ d'application du droit à l'oubli tel que prévu à l'article 17 du nouveau règlement. Nous envisagerons ensuite les obligations qui en découlent pour les responsables de traitement et finirons par commenter les issues possibles auxquelles cette nouvelle prérogative peut aboutir en pratique.

Section 1ère : Contenu et champ d'application

Le libellé de l'article 17 porte pour le moins à confusion. Intitulé « Droit à l'effacement », les termes « droit à l'oubli » sont accolés directement au titre et placés entre parenthèses[281]. Faut-il en conclure qu'il s'agit du même droit, ou que deux droits différents sont définis au sein du même article ? Le considérant 156 du règlement fait expressément référence au « droit à la rectification », « droit à l'effacement » et « droit à l'oubli ». De même, les considérants 65 et 66 mentionnent explicitement « le droit à l'oubli » et non pas « le droit à l'effacement ». Les débats précédant l'adoption de la version finale du règlement, rudement menés par le Comité des libertés civiles du Parlement européen notamment, démontrent l'importance de la

[275] Souligné par G. SARTOR, « The right to be forgotten in the Draft Data Protection Regulation », *International Data Privacy Law*, 2015, p. 64.
[276] V. REDING, « Privacy matters – Why the EU needs new personal data protection rules », SPEECH/10/700, discours prononcé à Bruxelles le 30 novembre 2010 dans le cadre de la *European Data Protection and Privacy Conference* : « *if people no longer want to use a service, they should have no problem wiping out their profiles*. »
[277] *Ibid.,* « *God forgives and forgets but the Web never does* ».
[278] Cécile de Terwangne présente d'ailleurs le nouvel article 17 comme un « droit de changer d'avis » ou « un droit au repentir ». *Voy*. C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit*., p. 247.
[279] C. TANKARD, « What the GDPR means for business », *Network Security*, 2016, n° 6, p. 5.
[280] *Voy*. art. 4, 1) du règlement 2016/679. L'identification pourra s'opérer directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
[281] La proposition de la Commission mentionnait initialement « *droit à l'oubli numérique* ». Le Parlement a par la suite modifié cette dénomination en « droit à l'effacement ». La version finale, après avoir été adoptée à la fois par le Parlement européen et le Conseil, nomme l'article 17 « *droit à l'effacement (« droit à l'oubli »)* ».

question pour certains. Une fois le règlement entré en application, l'éclairage de la Cour permettra sans doute de lever le voile sur cette incertitude juridique[282]. En attendant, nous plaidons en faveur de l'interprétation la plus simple qui soit vis-à-vis de ce problème terminologique : le droit à l'effacement et le droit à l'oubli devraient être considérés comme un seul et même droit, sans distinction juridique[283].

§1er : Quand peut-on réclamer un droit à l'oubli ?

Le premier paragraphe de l'article 17 établit une liste de six situations dans lesquelles « *la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant* ». En substance, celles-ci peuvent être résumées de la sorte :

a) *les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière* ;
b) la personne concernée retire son consentement sur lequel est fondé le traitement ;
c) la personne concernée s'oppose au traitement ;
d) les données ont fait l'objet d'un traitement illicite;
e) les données à caractère personnel doivent être effacées pour respecter une obligation légale;
f) les données ont été collectées dans le cadre d'une offre de services d'une société de l'information durant l'adolescence.

A. Traitement contraire au principe de finalité

Le premier cas renvoie à la violation du principe de finalité, lequel est à présent intégré à l'article 5, §1er, b) du règlement. Ce dernier reprend, au mot près, le principe énoncé à l'article 6, §1er, b) de la directive 95/46. Cependant, comme le souligne Giovanni Sartor, la formulation employée par l'article 17, §1er, a) laisse place à une certaine confusion. En effet, la finale de cette disposition ajoute « *ou traitée d'une autre manière* ». Faut-il dès lors

[282] C. CUIJPERS, E. KOSTA et N. PURTOVA, « Data Protection Reform and the Internet : The Draft Data Protection Regulation », Tilburg Law School Legal Studies research Paper Series n° 03/2014, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2373683 (16 mars 2016), p. 7.
[283] Certains commentateurs parle d'ailleurs de « droit à l'effacement et à l'oubli », ne faisant plus de distinction entre les deux. *Voy*. G. SARTOR, « The right to be forgotten in the Draft Data Protection Regulation », *op. cit*., p. 65.

conclure qu'à chaque fois que la finalité pour laquelle le traitement est effectué n'est pas identique à la finalité pour laquelle le traitement était initialement effectué, la condition est remplie ? Cela signifierait que le traitement de données effectué à des fins qui ne seraient pas *identiques* mais seulement *compatibles* avec la finalité pour laquelle le traitement était initialement effectué serait contraire à l'article 17, et permettrait à la personne concernée de demander l'effacement des données.

Une autre approche, que nous considérons comme étant la plus plausible, consisterait à considérer la condition comme étant remplie lorsque les données ne sont plus nécessaires à l'accomplissement des finalités pour lesquelles elles ont été collectées ou à l'accomplissement d'autres traitements compatibles avec ces finalités. Cette interprétation permettrait de calquer le nouveau régime sur celui qui prévaut actuellement dans la directive 95/46. Or, à la lecture du nouveau texte, nous n'avons pas trouvé d'éléments qui nous laisseraient penser que l'intention du législateur sur ce point était de s'écarter de l'ancien régime.

Néanmoins, force est de constater que le texte n'est pas clair et que de celui-ci naitront probablement des interprétations diverses.

B. Retrait du consentement

Le simple retrait du consentement comme raison juridiquement valable à la demande d'effacement des données est l'une des principales nouveautés du règlement[284]. Contrairement au régime actuel, il ne sera donc plus nécessaire de justifier sa demande d'effacement[285]. En revanche, il sera toujours possible pour le responsable de traitement d'invoquer un autre fondement juridique au traitement permettant de justifier celui-ci. Nous pensons par exemple à l'ensemble des exceptions prévues par le deuxième paragraphe de l'article 17.

En raison de la facilité avec laquelle il sera désormais possible de demander l'effacement de

[284] E. CAROLAN, « The continuing problems with online consent under the EU's emerging protection principles », *Computer Law & Security Review*, 2016, p. 470.
[285] Notons que ce droit au retrait du consentement était déjà formulé dans l'article 7, §3, du règlement 2016/679, qui dispose expressément que « *La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement*. »

ses données, il est fort à parier qu'en pratique, c'est sur ce fondement que la plupart des internautes obtiendront ce qu'ils réclament.

C. L'opposition au traitement

Toute personne concernée peut s'opposer à tout moment au traitement de ses données[286] lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public[287] ou aux fins des intérêts légitimes poursuivis par le responsable de traitement[288]. Si elle parvient à démontrer la particularité de sa situation[289], la personne concernée pourra alors exiger du responsable de traitement qu'il efface l'ensemble des données faisant l'objet du litige[290]. On notera à cet égard que l'article 6, §1er, f), *in fine*, exige de tenir particulièrement compte de l'âge de la personne concernée. Ainsi, il nous semble qu'un enfant ou un adolescent devrait plus facilement parvenir à prouver la particularité de sa situation. Sans doute devrait-il en être de même lorsque la personne concernée a consenti au traitement de ses données étant enfant ou adolescent.

Toutefois, le responsable de traitement se verra encore la possibilité de prouver qu'il existe des motifs légitimes et impérieux prévalant sur les intérêts et les droits et libertés de la personne concernée. Les critères établis par le G29 en marge de l'arrêt Google devraient à cet égard permettre aux autorités de contrôle d'apprécier de façon systématique et harmonisée la balance des intérêts entre les parties[291].

Malgré cette exception, le droit d'opposition devrait être plus facile à exercer pour la personne concernée qu'il ne l'est pour le moment[292]. Comme le souligne Cécile de Terwangne, « *cette inversion de la charge de la preuve doit être approuvée, car le responsable est en meilleure position pour connaître toutes les implications du*

[286] *Voy*. à cet égard l'article 21 du règlement 2016/679.
[287] Art. 6, §1er, e), du règlement 2016/679.
[288] Art. 6, §1er, f), du règlement 2016/679.
[289] Lors de son passage devant le Parlement européen en 2014, cette condition avait disparue. *Voy*. la proposition du parlement.
[290] La résolution du parlement en première lecture indiquait « *sans frais, à tout moment et sans autre justification, à titre général ou à toute fin spécifique* ». *Voy*. Résolution législative du Parlement européen 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), *P.E. Doc*., P7_TA 0212/2014 du 12 mars 2014, p. 1.
[291] *Voy*. l'opinion de Cécile de Terwangne : C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit*., p. 267.
[292] *Voy*. *supra* notre commentaire sur le droit d'opposition inséré dans la directive 95/46 à l'article 14.

traitement[293] ». Cette solution est également celle qu'avait retenue la Cour de justice de l'Union européenne qui semblait alors avoir instauré une sorte de *présomption de primauté* des droits de la personne concernée face aux intérêts économiques du responsable de traitement et de l'intérêt du public d'être informé[294].

Nous noterons enfin que lorsque les données sont traitées à des fins de prospection, la personne concernée a toujours le droit de s'opposer à tout moment à leur traitement et d'en demander l'effacement[295]. Il s'agit là d'une copie à peu près conforme à celle que l'on trouvait déjà dans l'article 14, §1,b) de la directive 95/46.

D. L'information a été collectée lorsqu'on était enfant dans le cadre de la société de l'information

L'article 17, §1er, f) mérite également une attention particulière. Absent de la proposition de la Commission et de la résolution du Parlement européen, cette disposition a pour objet les données personnelles diffusées dans le cadre de services de la société de l'information[296] durant la minorité. Elle s'inscrit dans une logique de protection accrue des mineurs lorsque ceux-ci sont confrontés à l'offre de services sur internet.

E. Les données ont fait l'objet d'un traitement illicite

L'article 17, §1er, d), est une sorte de catégorie résiduaire couvrant l'ensemble des traitements qui seraient illicites sur la base du droit à la protection des données personnelles[297]. Il faudra donc avoir égard à l'ensemble des principes listés à l'article 6 du règlement, ceux-ci étant, dans une large mesure, similaires à ceux listés à l'article 7 de la directive 95/46, mais également à toutes les autres conditions de licéité de traitement disséminées au sein du règlement.

---

[293] C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? », *op. cit*., p. 266.
[294] *Voy*. C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, points 81 et 97.
[295] La résolution du Parlement européen en 2014 prévoyait initialement que cela puisse se faire « *sans frais* ».
[296] L'article 1er, §1er, b), de la directive 2015/1535 les définis comme étant « *tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services* ». *Voy*. Dir (UE) n° 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.U.E*., L 241, du 17 septembre 2015, p. 1.
[297] G. SARTOR, « The right to be forgotten in the Draft Data Protection Regulation », *op. cit*., p. 66.

§2. Exception au droit à l'oubli : la liberté d'expression.

L'article 17, §3, établit une liste de cinq exceptions limitant le droit à l'effacement. Dans chacun de ces cas, le responsable du traitement ne sera ni tenu d'effacer les données ni d'informer les tiers des éventuelles corrections qu'il eut fallu apporter. Dans le cadre de notre étude, nous nous limiterons à l'analyse de la plus pertinente d'entre elles, eu égard aux questions qu'elle suscite. Les autres trouveront à s'appliquer dans des cas plus spécifiques[298].

L'exercice du droit à la liberté d'expression est la première exception prévue par l'article 17, § 3, a). On ne pourrait cependant en conclure que le législateur européen a voulu, par l'introduction de cette disposition, établir une « primauté absolue » du droit à la liberté d'expression face au droit à la protection des données. Une analyse au cas par cas devrait permettre de mettre en balance les différents droits fondamentaux en présence[299]. Cette conclusion fait d'ailleurs dire à Giovanni Sartor qu'il ne s'agit pas d'une réelle exception mais plutôt d'un moyen offert au responsable de légitimer ou de rendre licite le traitement qu'il opère[300]. Ainsi, l'insertion de la liberté d'expression comme exception au droit à l'effacement relèverait plus, à notre avis, de la mise en exergue, à des fins politiques, d'une valeur chère à l'Union, que d'un acte délibéré destiné à produire des effets juridiques limitant drastiquement le droit à l'effacement.

Notons enfin que cette disposition doit être lue en combinaison avec l'article 85 du règlement. Ce dernier exige des États membres qu'ils « *concilient, par la loi, le droit à la protection des données à caractère personnel* […] *et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire*[301] ». Ceux-ci sont, dans ce cadre, expressément autorisés à prévoir des exemptions ou des dérogations au règlement afin de concilier ces deux droits fondamentaux[302]. Cela doit toutefois se faire sous réserve d'en notifier la Commission européenne[303].

Cette approche est, selon nous, critiquable. En effet, le choix d'adopter un règlement plutôt

[298] Les autres exceptions sont relatives au respect d'une obligation légale, à des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ou à la contestation, l'exercice ou la défense de droits en justice.
[299] C'est d'ailleurs ce que suggère le considérant 4 du règlement 2016/679.
[300] G. SARTOR, « The right to be forgotten in the Draft Data Protection Regulation », *op. cit*., p. 67.
[301] Art. 85, §1er, du règlement 2016/679.
[302] Art. 85, §2, du règlement 2016/679. Le considérant 153 du règlement vise plus spécifiquement le domaine de l'audiovisuel et les documents d'archives d'actualités et bibliothèques de la presse.
[303] Art. 85, §3, du règlement 2016/679.

qu'une directive avait pour but de réduire au maximum les risques de divergences dans l'application des nouvelles normes entre les États membres[304]. Force est de constater que la latitude qui leur est aujourd'hui octroyée risque de conduire à l'adoption de règles plus ou moins en faveur de la liberté d'expression ou de la protection des données, en fonction de la culture juridique de chaque État[305]. Peut-être aurait-il été opportun de faire usage des critères déjà établis par le G29[306] afin d'encadrer et d'harmoniser quelque peu la balance d'intérêts que devront effectuer les législateurs et les Cours et tribunaux nationaux.

Section 2 : Quelles sont les sanctions en cas de contravention au règlement ?

Comme nous l'avons vu précédemment, le droit à l'oubli, tel que nouvellement formulé dans le règlement 2016/679, prend la forme d'un droit à l'effacement, ou, plus précisément, le droit d'exiger du responsable de traitement qu'il supprime les données personnelles de la personne concernée. Ce droit peut être exercé directement auprès du responsable et, en cas de refus, mis en œuvre par l'intermédiaire des autorités nationales de protection des données[307].

Afin d'assurer la mise en œuvre de ce droit, le législateur a notamment prévu la possibilité de demander la réparation du préjudice[308] matériel ou moral éventuellement subi par un traitement illicite des données personnelles[309]. A l'instar de l'ancien régime, cette obligation de réparer s'inscrit dans une logique de responsabilité conjointe (avec possibilité d'une action récursoire lorsqu'un seul des responsables est amené à réparer *effectivement* le dommage[310]). Ainsi, « *tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du* […] *règlement*[311] ». De même, des sanctions administratives sont prévues en cas de non respect du droit à l'oubli. Des amendes pouvant s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire annuel

[304] C. KUNER, « The European Commission's Proposed Data Protection Regulation : A Copernican Revolution in European Data Protection Law », *Bloomberg BNA Privacy and Security Law Report*, 2012, p. 3.
[305] A cet égard, le considérant 153 du règlement 2016/679 ajoute que « *lorsque ces exemptions ou dérogations diffèrent d'un État membre à l'autre, le droit de l'État membre dont relève le responsable du traitement devrait s'appliquer*. »
[306] Groupe de travail « Article 29 » sur la protection des données, « Guidelines on the implementation of the Court of Justice of the European Union judgement on Google Span and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González C-131/12 », 26 novembre 2014, 14/EN WP 225.
[307] Art. 58, § 2, c) et g), du règlement 2016/679.
[308] Le considérant 75 du règlement 2016/679 donne à titre d'exemple les cas de discrimination, de vol ou d'atteinte à la réputation.
[309] Art. 82 du règlement 2016/679.
[310] Art. 82, §5, du règlement 2016/679.
[311] Art. 82, §4, du règlement 2016/679

mondial total de l'entreprise responsable du traitement pourront être administrées[312]. Ces sanctions très sévères[313] ont d'ailleurs déjà fait dire à certains qu'elles encourageront les entreprises à donner raison aux personnes concernées plutôt que de vérifier que les conditions liées à la demande d'effacement soient remplies[314].

Section 3: L'obligation de notification aux tiers.

Parmi les obligations les plus contraignantes du nouveau règlement, l'obligation de notifier aux tiers les corrections apportées aux données est sans nul doute l'une des plus remarquables[315]. L'article 17, §2, dispose en effet que « *lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer* […], *le responsable de traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables de traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci*. »

Comme le suggère le texte, il s'agit toutefois d'une *obligation de moyen* et non pas *de résultat*. Gabriela Zanfir[316] renvoie en ce sens aux principes UNIDROIT, et plus particulièrement à l'article 5.1.4 de ces principes, lequel exige d'une partie soumise à une obligation de moyen qu'elle mette en œuvre autant de moyens que l'aurait fait une autre personne de même nature placée dans les mêmes circonstances. Appliqué au contexte de l'article 17, §2, et par opposition à l'article 17, §1er, qui, lui, fait état d'une obligation de résultat, un responsable de traitement ne sera pas nécessairement sanctionné s'il ne parvient pas à informer l'ensemble des responsables de traitement qui traitent les données de la personne concernée. Il pourra notamment invoquer l'impossibilité de satisfaire à ses

[312] Art. 83, §5, du règlement 2016/679.
[313] Paul De Hert constate l'absence de sanctions pénales dans le règlement. Le choix du législateur s'est ainsi plutôt orienté vers des considérations économiques, les amendes administratives étant plus faciles à mettre en œuvre et plus dissuasives à l'égard de poids lourds tels que Google. *Voy*. P. DE HERT, « The EU data protection reform and the (forgotten) use of criminal sanctions », *International Data Privacy Law*, 2014, p. 264.
[314] I. SPAHIU, « Between the right to know and the right to forget : looking beyond the Google case », *op. cit*., p. 4.
[315] M. BURRI et R. SCHÄR, « The Reform of the EU Data Protection Framework : Outlining Key Changes and Assessing Their Fitness for a Data-driven Economy », 2016, p. 14, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792222 (12 juin 2016) ; P. DE HERT et V. PAPAKONSTANTINOU, « The new General Data Protection Regulation : Still a sound system for the protection of individuals ? », *Computer Law & Security Review*, 2016, p. 188.
[316] G. ZANFIR, « Tracing the Right to Be Forgotten in the Short History of Data Protection Law : The New Clothes of an Old Right », p. 236.

obligations dû à des raisons techniques (il ne dispose pas des technologies nécessaires) ou à des coûts de mise en œuvre trop élevés. Cette dernière justification sera particulièrement intéressante pour les moteurs de recherche qui risquent d'être fortement impactés par cette obligation. Une comparaison entre les différents acteurs du secteur (tels que Bing, Yahoo ! ou Google) permettra d'évaluer de manière plus précise ce en quoi consiste « *une obligation de moyen* » pour chacun d'entre eux.

Enfin, on remarquera que cette obligation d'information à l'égard des tiers responsables était déjà prévue par l'article 12, c), de la directive 95/46. Cependant, les responsables de traitement n'y étaient tenu que dans la mesure où cela n'était pas impossible ou ne supposait pas un effort disproportionné. En pratique cependant, le contexte du numérique et de l'internet a rapidement permi de contourner cette obligation en la désignant comme disproportionnée[317].

[317] *Ibid*., p. 243.

Conclusion

Le droit à l'oubli est une réalité devenue nécessaire, spécialement au regard de notre conception européenne du droit à la vie privée. Les difficultés liées à l'ubiquité de l'Internet ont obligé le législateur européen à adopter des mesures qui, par la force des choses, s'appliquent à des entités établies à l'étranger. A cet égard, nous plaidons, à l'instar de Susan Corbett[318], pour l'entretien de négociations au niveau international. La problématique étant susceptible de toucher n'importe quel citoyen du monde ayant accès à une connexion Internet, c'est en effet une solution globale, et non pas exclusivement européenne, qu'il faudra trouver dans le futur.

Nous avons également mis en lumière les lacunes que comporte le régime actuel du droit à l'oubli. L'absence d'indications plus précises quant à la durée de vie potentielle des données est source d'incertitude juridique, même si la méthode au cas par cas actuellement utilisée par les autorités nationales de protection des données semble être relativement efficace. Les nouvelles lignes directrices publiées à la suite de l'arrêt Google Spain par le G29 devraient, à cet égard, permettre d'harmoniser quelque peu les critères sur base desquels les responsables de traitement et les autorités nationales abordent les demandes d'effacement.

De même, la question de l'équilibre à entretenir entre les droits fondamentaux restera, malgré l'entrée en vigueur du nouveau règlement relatif à la protetcion des données, l'un des enjeux les plus cruciaux. L'introduction de la liberté d'expression comme exception à l'exercice du droit à l'oubli souligne la volonté politique de l'Union de maintenir sur un même pied d'égalité les droits reconnus par la Charte européenne. A nouveau, seule une analyse au cas par cas, avec l'aide de la jurisprudence que nous avons tenté de traiter dans cette étude, permettra de partager les intérêts opposés des personnes concernées et des reponsables de traitement. Nul doute cependant que les Cours et tribunaux européens continueront à mettre en balance ces intérêts de manière appropriée, comme ils l'ont toujours fait dans cette longue tradition juridique qu'est la nôtre.

Enfin, il convient de souligner les éclairements apportés par le nouveau règlement. Si celui-ci ne crée pas fondamentalement de nouveu droit, il a le mérite de clarifier les contours du droit à l'oubli et de renforcer le droit à l'effacement.

[318] S. CORBETT, « The retention of personal information online ; A cal for international regulation of privacy law », *Computer Law & Security Review*, 2013, pp. 246-254.

Bibliographie

Législation

- Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950.

- Charte des droits fondamentaux de l'Union européenne, C 364, *J.O.C.E.*, 18 décembre 2000, p. 1.

- Règl. (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/47/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, du 4 mai 2016, p. 1.

- Dir. (CE) n° 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281, du 23 novembre 1995, p. 31.

- Dir. (CE) n° 2006/24 du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.C.E.*, L 105, du 13 avril 2006, p. 54.

- Dir (UE) n° 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.U.E.*, L 241, du 17 septembre 2015, p. 1.

- 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 et à la libre circulation de ces données (règlement général sur la protection des données), *C.O.M.* (2012) 11 final.

- Résolution législative du Parlement européen 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), *P.E. Doc.*, P7_TA 0212/2014 du 12 mars 2014, p. 1.

Jurisprudence

Union européenne

- C.J.C.E., 20 mai 2003 (Österreichischer Rundfunk e.a.), C-465/00, C-138/01 et C-139/01, http://www.curia.europa.eu (13 mars 2016).

- C.J.C.E., 6 novembre 2003 (Bodil Lindqvist), C-101/01, http://www.curia.europa.eu (14 juin 2016).

- C.J.U.E., 16 décembre 2008 (*Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*), C-73/07, http://www.curia.europa.eu (14 juin 2016).

- C.J.U.E., 13 mai 2014 (Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González), C-131/12, concl. Av. gén. N. JÄÄSKINEN, http://www.curia.europa.eu (16 novembre 2014).

- C.J.U.E., 11 décembre 2014 (František Ryneš c. Úřad pro ochranu osobních údajů), C-212/13, http://www.curia.europa.eu (14 juin 2016).

- C.J.U.E., 1er octobre 2015 (Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság), C-230/14, http://www.curia.europa.eu (14 juin 2016).

Conseil de l'Europe

- Cour eur. D.H., arrêt Peck c. Royaume-Uni du 28 janvier 2003, http://echr.coe.int (14 avril 2016).

- Cour eur. D.H., arrêt I. c. Finlande du 17 juillet 2008, http://echr.coe.int (19 juin 2016).

- Cour eur. D.H., arrêt K.U. c. Finlande du 2 décembre 2008, http://echr.coe.int (19 juin 2016).

- Cour eur. D.H., arrêt S. et Marper c. Royaume-Uni du 4 décembre 2008, http://echr.coe.int (19 juin 2016).

- Cour eur. D.H., arrêt Aleksey Ovchinnikov c. Russie du 16 décembre 2010, http://echr.coe.int (19 juin 2016).

- Cour eur. D.H., arrêt Von Hannover c. Allemagne du 7 février 2012, http://echr.coe.int (19 juin 2016).

- Cour eur. D.H., arrêt Axel Springer AG c. Allemagne du 7 février 2012, http://echr.coe.int (19 juin 2016).

- Cour eur. D.H., arrêt Węgrzynowski et Smolczewski c. Poland du 16 juillet 2013, point 58, http://echr.coe.int (19 juin 2016).

Doctrine

Monographies

- BYGRAVE L.A., *Data Protection Law. Approaching its Rationale, Logic and Limits*, The Hague, London, New York, Kluwer Law International, 2002.

- DE BOT D., *Verwerking van persoonsgegens*, Antwerpen, Kluwer, 2002.

- DOCQUIR B., *Le droit de la vie privée*, Bruxelles, De Boeck, Larcier, 2008.

- FLORIDI L., *Protection of Information and the Right to Privacy — A New Equilibrium ?*, Cham, Heidelberg, New York, Dordrecht, London, Springer, 2014.

- GONZALEZ FUSTER G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, Heidelberg, New York, Dordrecht, London, Springer, 2014.

- HONDIUS F.W., *Emerging data protection in Europe*, Amsterdam, Oxford, North-Holland/American Elsevier, 1975.

- KINDT E.J., *Privacy and DataProtection Issues of Biometric Applications — A Comparative Legal Analysis*, Dordrecht, Heidelberg, New York, London, Springer, 2013.

- KLABBERS J., *International Law*, Cambridge, Cambridge University Press, 2013.

- KOHL U., *Jurisdiction and the Internet. Regulatory Competence over Online Activity*, Cambridge, Cambridge University Press, 2010.

- KORFF D., *Data Protection Laws in the European Union*, Federation of European Direct Marketing & Direct Marketing Association, 2005.

- KUNER C., *European Data Protection Law. Corporate Compliance and Regulation*, 2nd Edition, Oxford, Oxford University Press, 2007.

- LAFFAIRE M.-L., *Protection des données à caractère personnel*, Paris, Éditions d'Organisation, 2005.

- LOPEZ-TARRUELLA A., *Google and the Law — Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, The Hague, Springer, 2012.

- MAYER-SCHÖNBERGER V., *Delete : The Virtue of Forgetting in the Digital Age*, Princeton, Princeton University Press, 2009.

- NUGTER A.C.M., *Transborder Flow of Personal Data within EC*, Amsterdam, Springer, 1990.

- PRECHAL S., *Directives in EC Law*, Oxford, Oxford University Press, 2005.

- SIEMEN B., *Datenschutz als europäisches Grundrecht*, Berlin, Duncker & Humblot, 2006.

- SIMITIS S., *Collected courses of the Academy of European Law*, Vol. VIII-1, The Hague, Kluwer Law International, 1997.

- VIOLA DE AZEVEDO CUNHA M., *Market Integration Through Data Protection — An Analysis of the Insurance and Financial Industries in the EU*, Dordrecht, Heidelberg, New York, London, Springer, 2013.

- WALRAVE M., *Privacy Gescand? Direct marketing en de bescherming van de persoonlijke levenssfeer*, Leuven, Universitaire Pers Leuven, 1999.

- ZITTRAIN J.L., *The Future of the Internet and How to Stop It*, New Haven, London, Yale University Press, 2008.

Articles de périodiques

- ABRAMSON J., « Searching for Reputation : Reconciling Free Speech and the Right To Be Forgotten », *North Carolina Journal of Law & Technology*, 2015, Vol. 17, n° 1, pp. 1-78.

- AMBROSE M.L., « It's About Time : Privacy, Information Life Cycles, and the Right to be Forgotten », *Stanford Technology Law Review*, 2013, Vol. 16, n° 2, pp. 369-422.

- AMBROSE M.L. et AUSLOOS J., « The Right To Be Forgotten Across The Pond », *Journal of Information Policy*, 2013, Vol. 3, pp. 1-23.

- ARAMAZANI A., « Le droit à l'oubli et internet », *R.D.T.I.*, 2011, pp. 34-49.

- AUSLOOS J., « The Right to be Forgotten — Worth Remembering ? », *Computer Law & Security Review*, 2012, pp. 143-152.

- AUSLOOS J., GRAUX H. et VALCKE P., « The Right to be Forgotten in the Internet Era », *ICRI Working Paper Series*, 2012, n°11.

- AUSLOOS J., KUCZERAWY A. et VAN ALSENOY B., « Search engines after Google Spain : internet@liberty or privacy@peril? », KU Leuven ICRI Working Paper Series

n° 15/2013, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494 (17 février 2015).

- BAGGER TRANBERG C., « Proportionality and data protection in the case law of the European Court of Justice », *International Data Privacy Law*, 2011, pp. 239-248.

- BALBONI P., COOPER D., IMPERIALI R. et MACENAITE M., « Legitimate interest of the data controller — New data protection paradigm : legitimacy grounded on appropriate protection », *International Data Privacy Law*, 2013, pp. 244-261.

- BARTOLINI C. et SIRY L., « The right to be forgotten in the light of the consent of the data subject », *Computer Law & Security Review*, 2016, pp. 218-237.

- BASSINI M. et POLLICINO O., « Reconciling the right to be forgotten and freedom of information in the digital age. Past and future of personal data protection in the EU », 2013, http://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wccl-cmdc/wccl/papers/ws14/w14-Pollicino&Bassini.pdf (12 octobre 2014).

- BENNETT S.C., « The Right to Be Forgotten : Reconciling EU and US Perspectives », *Berkeley Journal of International Law*, 2012, Vol. 30, n° 1, pp. 161-195.

- BERNAL P.A., « A Right to Delete ? », *E.J.L.T.*, 2011, Vol. 2, n°2, pp. 1-18.

- BERNARD-GLANZ C., « Les arrêts Digital Rights Ireland et Google Spain, ou le printemps européen de la protection des données », *C.D.E.*, 2014, pp. 685-717.

- BLUME P., « The myths pertaining to the proposed General Data Protection Regulation », *International Data Privacy law*, 2014, pp. 269-273.

- BOULANGER M.-H., DE TERWANGNE C., LÉONARD T., LOUVEAUX S., MOREAUX D. et POULLET Y., « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.*, 1997, pp. 121-127.

- BOLTON R.L., « The Right To Be Forgotten : Forced Amnesia in a Technological Age », *Journal of Information Technology & Privacy Law*, 2014, Vol. 31, pp. 133-144.

- BRUENING P., CARTER S. et HOFFMAN D., « The Right to Obscurity : How We Can Implement the Google Spain Decision », *North Carolina Journal of Law & Technology*, 2016, Vol. 17, n° 3, pp. 437-481.

- BRUGUIÈRE J.-M., « Le droit à l'oubli numérique, un droit à oublier », *D. (D.S.)*, 2014, pp. 299-204.

- BUNN A., « The curious case of the right to be forgotten », *Computer Law & Security Review*, 2015, pp. 336-350.

- BURRI M. et SCHÄR R., « The Reform of the EU Data Protection Framework : Outlining Key Changes and Assessing Their Fitness for a Data-driven Economy », 2016, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792222 (12 juin 2016)

- BUTLER O., « The Expanding Scope of the Data Protection Directive : The Exception for a Purely Personal or Household Activity », University of Cambridge Faculty of Law Research Paper n° 54/2015, 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2660916 (12 juin 2016).

- BYGRAVE L.A., « European Data Protection – Determining Applicable Law Pursuant to European Data Protection Legislation », *Computer Law & Security Review*, 2000, pp. 252-257.

- CARBONE C.E., « To Be or Not To Be Forgotten : Balancing the Right to Know with the Right to Privacy in the Digital Age », *Virginia Journal of Social Policy & the Law*, 2015, Vol. 22, n° 3, pp. 525-560.

- CAROLAN E., « The continuing problems with online consent under the EU's emerging protection principles », *Computer Law & Security Review*, 2016, pp. 462-473.

- CASTELLANO P.S., « The right to be forgotten under European Law : Constitutional debate », *Lex Electronica*, Vol. 16, n° 1, pp. 1-30.

- CASTETS-RENARD C. et VOSS W.G., « Proposal for an International Taxonomy on the Various Forms of the « Right to Be Forgotten » : A Study on the Convergence of Norms », *Colorado Technology Law Journal*, 2016, n°14, pp. 281-344.

- CATE F.H., KUNER C., LYNSKEY O., MILLARD C. et SVANTESSON D.J.B., « When two worlds collide : the interface between competition law and data protection », *International Data Privacy Law*, 2014, pp. 247-248.

- CIAVARELLA R. et DE TERWANGNE C., « Online Social Network and Young People's Privacy Protection : The Role of the Right to Be Forgotten », *in Minding Minors Wandering the Web : Regulating Online Child Safety* (sous la dir. de S. VAN

DER HOF, B. VAN DEN BERG et B. SCHERMER), The Hague, Springer, 2014, pp. 157-171.

- COFONE I., « Google v. Spain : A Right To Be Forgotten ? », *Chicago-Kent Journal of International and Comparative Law*, 2015, Vol. 15, pp. 1-11.

- COLONNA L., « Data Mining and Its Paradoxical Relationship to the Purpose Limitation Principle », *in Reloading Data Protection – Multidisciplinary Insights and Contemporary Challenges* (sous la dir. de P. DE HERT, S. GUTWIRTH et R. LEENES), Dordrecht, 2014, pp. 299-321.

- CORBETT S., « The retention of personal information online ; A cal for international regulation of privacy law », *Computer Law & Security Review*, 2013, pp. 246-254.

- CRUYSMANS E., « Liberté d'expression, archives numériques et protection de la vie privée : la conciliation de trois réalités divergentes grâce au droit à l'oubli », *J.L.M.B.*, 2014, pp. 1972-1980.

- CRUYSMANS E., « Un droit à l'oubli face aux moteurs de recherche : droit applicable et responsabilité pour le référencement de données inadéquates, non pertinentes ou excessives », *J.T.*, 2014, pp. 457-459.

- CUIJPERS C., KOSTA E. et PURTOVA N., « Data Protection Reform and the Internet : The Draft Data Protection Regulation », Tilburg Law School Legal Studies research Paper Series n° 03/2014, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2373683 (16 mars 2016).

- DEFREYNE E., « Le droit à l'oubli et les archives journalistiques », *R.D.T.I*, 2013, pp. 75-98.

- DE HERT P., « The EU data protection reform and the (forgotten) use of criminal sanctions », *International Data Privacy Law*, 2014, pp. 262-268.

- DE HERT P. et GUTWIRTH S., « Data Protection in the Case Law of Strasbourg and Luxembourg : Constitutionalisation in Action », *in Reinventing Data Protection ?* (sous la dir. de P. DE HERT, C. DE TERWANGNE, S. GUTWIRTH et S. NOUWT), Dordrecht, Springer, 2009, pp. 3-44.

- DE HERT P. et PAPAKONSTANTINOU V., « The new General Data Protection Regulation : Still a sound system for the protection of individuals ? », *Computer Law & Security Review*, 2016, pp. 179-194.

- DE HERT P. et PAPKONSTANTINOU V., « The proposed data protection Regulation replacing Directive 95/46/EC : A sound system for the protection of individuals », *Computer Law & Security Review*, 2012, pp. 130-142.

- DE SCHUTTER O. et TULKENS F., « Rights in Conflict : the European Court of Human Rights as a Pragmatic Institution », *in Conflicts Between Fundamental Rights* (sous la dir. de E. BREMS), Antwerpen, Oxford, Portland, Intersentia, 2008, pp. 169-216.

- DE TERWANGNE C., « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *R.D.T.I.*, 2004, pp. 81-99.

- DE TERWANGNE C., « 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 », *in Enjeux européens et mondiaux de la protection des données personnelles* (sous la dir. de A. GROSJEAN), Bruxelles, Larcier, 2016, pp. 245-275.

- DE TERWANGNE C., « Internet Privacy and the Right to Be Forgotten/Right to Oblivion », *Revista de Internet, Derecho y Política*, 2012, pp. 109-121.

- DOUGLAS M., « Questioning the Right To Be Forgotten », *Alternative Law Journal*, 2015, Vol. 40, n° 2, pp. 109-112.

- DOUWE K., « EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws », 2002, http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE (19 mars 2016).

- DUMORTIER J., KOSTA E., KUCZERAWY A. et LEENES R., « Regulating Identity Management », *in Digital Privacy. PRIME — Privacy and Identity Management for Europe* (sous la dir. de J. GAMENISH, R. LEENES et D. SOMMER), Berlin, Heidelberg, Springer, 2011, pp. 73-90.

- DUNCAN L'HOIRY X. et NORRIS C., « The honest data protection officier's guide to enable citizens to exercise their subject access rights : lessons from a ten-country European study », *International Data Privacy Law*, 2015, pp. 190-204.

- DUPONT-LASSALE J., « Beaucoup de bruit pour rien ? La précarité du droit à l'oubli numérique consacré par la Cour de justice de l'Union européenne dans l'affaire Google Spain », *Rev. trim. D.H.*, 2015, pp. 987-1019.

- ERDOS D., « Confused ? Analysing the Scope of Freedom of Speech Protection vis-à-vis European Data Protection », University of Oxford Legal Research Paper Series, Paper n° 48/2012, 2012, pp. 1-36, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2119187 (17 mars 2016).

- ESAYAS S.Y., « The rôle of anonymisation and pseudonymisation under the EU data rules : beyond the all or nothing approach », *E.J.L.T*, 2015, pp. 1-28.

- FAIRCHILD A., KOSTA E., LEENES R. et PRIEM B., « The Need for Privacy-Enhancing Identity Management », *in Digital Privacy. PRIME – Privacy and Identity Management for Europe* (sous la dir. de J. GAMENISH, R. LEENES et D. SOMMER), Berlin, Heidelberg, Springer, 2011, pp. 53-72.

- FAZLIOGLU M., « Forget me not : the clash of the right to be forgotten and freedom of expression on the Internet », *International Data Privacy Law*, 2013, pp. 149-157.

- FOEGLE J.-Ph., « La CJUE, magicienne européenne du droit à l'oubli numérique », *La Rev. D.H.*, 2014, https://revdh.revues.org/840 (1er juillet 2016).

- FORD M., « Will Europe Censor This Article? », The Atlantic, 13 mai 2014, http://www.theatlantic.com/international/archive/2014/05/europes-troubling-new-right-to-be-forgotten/370796/ (14 novembre 2015).

- FORDE A., « Implications of the Right To Be Forgotten », *Tulane Journal of Technology & Intellectual Property*, 2015, pp. 83-131.

- GAYREL C., HERVEG J. et VAN GYSEGHEM J.-M., « La protection des données à caractère personnel en droit européen », *J.E.D.H.*, 2015, pp. 57-84.

- GEORGE D. et TAMO A., « Oblivion, Erasure and Forgetting in the Digital Age », *J.I.P.I.T.E.C.*, 2014, pp. 71-87.

- GEORGE D. et TAMO A., « Ein Europäisches Recht auf Vergessen – eine Schweizer Pflicht zum Löschen? — Thesen zum möglichen Einfluss von Art. 17 des DSG-VO Entwurfes auf multinationale Unternehmen in der Schweiz », *in Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft* (sous la dir. de S. BRÄNDLI, R. SCHISTER et A. TAMO), Bern, 2013, pp. 31-56.

- GOMES DE ANDRADE N.N., « Oblivion : The Right to Be Different… from Oneself — Reproposing the Right to Be Forgotten », *Revista de Internet, Derecho y Política,* 2012, pp. 122-137.

- HARDY B., « Application dans l'espace de la directive 95/46/CE : la géographie du droit à l'oubli », *Rev. trim. dr. europ.*, 2014, pp. 879-897.

- HEYWOOD D. et REES C., « The right to be forgotten or the principle that has been remembered », *Computer Law & Security Review*, 2014, pp. 574-578.

- HOVEN M., « Balancing Privacy and Speech in the Right to Be Forgotten », *Harvard Journal of Law & Technology*, 2012, http://jolt.law.harvard.edu/digest/privacy/balancing-privacy-and-speech-in-the-right-to-be-forgotten (18 octobre 2015).

- JACOBS D. et ROTTENBERG M., « Updating the Law of Information Privacy : The New Framework of the European Union », *Harvard Journal of Law & Public Policy*, 2013, Vol. 36, n° 2, pp. 605-652.

- KAMPMARK B., « To Find or be Forgotten : Global Tensions on the Right to Erasure and Internet Governance », *Journal of Global Faultlines*, 2015, Vol. 2, n° 2, pp. 1-18.

- KERR J., « What is a Search Engine ? The Simple Question the Court of Justice of the European Union Forgot to Ask and What It Means for the Future of the Right to be Forgotten », *Chicago Journal of International Law*, 2016, Vol. 17, n°1, pp. 217-243.

- KNEZ R., « Right to Be Forgotten — Indeed a New Personal Right in Digital EU Market ? », *Journal for the International and european law, economics and market integrations*, 2016, Vol. 3, n° 1, pp. 31-44.

- KOEKKOEK M. et VAN ALSENOY B., « Internet and jurisdiction after Google Spain : the extraterritorial reach of the right to be delisted », *International Data Privacy Law*, 2015, pp. 105-120.

- KOHL U., « Barbarians in Our Midst : Cultural Diversity on the Transnational Internet », *E.J.L.T.*, 2014, Vol. 5, n° 1, pp. 1-32.

- KOKOTT J. et SOBOTTA C., « The Charter of Fundamental Rights of the European Union After Lisbon », EUI Working Paper AEL, European University Institute, 2010, n° 6, http://cadmus.eui.eu/bitstream/handle/1814/15208/AEL_WP_2010_06.pdf?sequence=3&isAllowed=y (13 mars 2016).

- KOOPS B.-J., « Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right To Be Forgotten in Big Data Practice », *SCRIPTed*, Vol.8, n° 3, 2011.

- KULEVSKA S. et RUSTAD M.L., « Reconceptualizing the Right To Be Forgotten To Enable Transatlantic Data Flow », *Harvard Journal of Law & Technology*, 2015, Vol. 28, n°2, pp. 349-417.

- KULK S. et ZUIDERVEEN BORGESIUS F., « Freedom of Expression and Right to Be Forgotten Cases in the Netherlands After Google Spain », *E.D.P.L.*, 2015, Vol. 2, pp. 113-124.

- KUNER C., « The European Commission's Proposed Data Protection Regulation : A Copernican Revolution in European Data Protection Law », *Bloomberg BNA Privacy and Security Law Report*, 2012, pp. 1-15.

- KUNER C., « Data protection Law and International Jurisdiction on the Internet (Part 1) », *International Journal of Law and Information Technology*, 2010, pp. 176-193.

- LE CLAINCHE J., « L'adaptation du « droit à l'oubli » au contexte numérique », *R.E.D.C.*, 2012, pp. 39-60.

- LEE E., « Recognizing Rights in Real Time : The Role of Google in the EU Right to Be Forgotten », *University of California Davis Law Review*, 2016, Vol. 49, pp. 1017-1095.

- LIDDICOAT J., « The Right To Be Forgotten », Presentation during Privacy Week 2015 at the IT and Oline Law Conferences in Auckland on 7 May and Wellington on 8 May, 2015, https://www.privacy.org.nz/news-and-publications/speeches-and-presentations/the-right-to-be-forgotten-paper/ (12 juin 2016).

- LIPTON J.D. et SANCHEZ ABRIL P., « The Right to be Forgotten : Who Decides What the World Forgets ? », *Kentucky Law Journal*, 2015, Vol. 103, pp. 363-389.

- MANTELERO A., « Competitive value of data protection : the impact of data protection regulation on online behaviour », *International Data Privacy Law*, 2013, pp. 229-238.

- MANTELERO A., « The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten », *Computer Law & Security Review*, 2013, pp. 229-235.

- MARKOU C., « The Right to Be Forgotten : Ten Reasons Why It Should Be Forgotten », *in Reforming European Data protection Law* (sous la dir. de P. DE HERT, S. GUTWIRTH et R. LEENES), Dordrecht, 2015, pp. 203-226.

- MAXWELL W.J., « Principles-based regulation of personal data : the case of fair processing », *International Data Privacy Law*, 2015, pp. 205-216.

- MAYER-SCHÖNBERGER V., « Useful Void : The Art of Forgetting in the Age of Ubiquitous Computing », Working Paper, John F. Kennedy School of Government, Harvard University, 2007.

- MOEREL L., « Back to basics : when does EU data protection law apply ? », *International Data Privacy Law*, 2011, pp. 92-110.

- MOEREL L., « The long arm of Eu data protection law : Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide ? », *International Data Privacy Law*, 2011, pp. 28-46.

- MOINY J.-F., « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010, pp. 235-271.

- MONTERO E. et VAN ENIS Q., « Les métamorphoses du droit à l'oubli », *R.G.D.C.*, 2016, pp. 243-255.

- NISSENBAUM H. et TOUBIANA V., « Analysis of Google Logs Retention Policies », *Journal of Privacy and Confidentiality*, 2011, Vol. 3, n° 1, pp. 3-26.

- O'HARA K., « The Right to Be Forgotten : The Good, the Bad, and the Ugly », *IEEE Internet Computing*, 2015, Vol. 19, n° 4, pp. 73-79.

- O'HARA K., SHADBOLT N. et HALL W., « A Pragmatic Approach To The Right To Be Forgotten », Global Commission on Internet Governance, Paper Series n°26, 2016, http://eprints.soton.ac.uk/389777/1/GCIG%20no26%20web.pdf (12 juin 2016).

- O'HARA K. et SHADBOLT N., « The Right to be Forgotten : Its Potential Rôle in a Coherent Privacy Regime », *Eur. Data Prot. L. Rev.*, 2015, n° 3, pp. 178-189.

- PADOVA Y., « What the European Draft regulation on Personal Data is going to change for companies », *International Data Privacy Law*, 2014, pp. 39-52.

- PEASE A., « The Right to Be Forgotten : Asserting Control over our Digital Identity or Re-Writing History ? », IRPPS Working Paper Series n° 83/2015, 2015.

- PEROTTI E., « The European Ruling on the Right to be Forgotten and its extra-EU implementation », 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703325 (13 avril 2016).

- PEYROU S., « Un nouveau cadre juridique général pour la protection des données au sein de l'Union européenne : une réforme législative ambitieuse », *R.A.E.*, 2012, pp. 149-162.

- POULLET Y., « The Directive 95/46/EC : Ten years after », *Computer Law & Security Report*, 2006, pp. 206-217.

- POULLET Y. et ROUVROY A., « The Right to Informational Self-Determination and the Value of Self-Development : Reassessing the Importance of Privacy for Democracy », *in Reinventing Data Protection ?* (sous la dir. de P. DE HERT, C. DE TERWANGNE, S. GUTWIRTH et S. NOUWT), Dordrecht, Springer, 2009, pp. 45-76.

- PURTOVA N., « Default entitlements in personal data in the proposed Regulation : Informational self-determination off the table… and back on again ? », *Computer Law & Security Review*, 2014, pp. 6-24.

- REDING V., « Privacy matters – Why the EU needs new personal data protection rules », SPEECH/10/700, discours prononcé à Bruxelles le 30 novembre 2010 dans le cadre de la *European Data Protection and Privacy Conference*.

- ROSEN J., « Symposium Issue. The Right To Be Forgotten », *Stanford Law Review Online*, Vol. 64, 2012, pp. 88-92.

- ROUVROY A., « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information », version augmentée du chapitre paru dans *La sécurité de l'individu numérisé – Réflexions prospectives et internationales*, Paris, L'Harmattan, 2008, pp. 249-278.

- SARTOR G., « The right to be forgotten in the Draft Data Protection Regulation », *International Data Privacy Law*, 2015, pp. 64-72.

- SARTOR G., « Providers' liabilities in the new EU Data Protection Regulation : A threat to Internet freedoms ? », *International Data Privacy Law*, 2013, pp. 3-12.

- SAVIRIMUTHU J. et WONG R., « All or Nothing : This is the Question ? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet », *John Marshall Journal of Computer & Information Law*, 2008, Vol. 25, pp. 241-266.

- SCHWARTZ P.M., « Property, Privacy, and Personal Data », *Harvard Law Review*, 2004, Vol. 117, n° 7, pp. 2056-2128.

- SHOOR E.A., « Narrowing the Right to be Forgotten : Why the European Union needs to amend the Proposed Data Protection Regulation », *Brooklyn Journal of International Law*, 2014, Vol. 39, n° 1, pp. 487-519.

- SPAHIU I., « Between the right to know and the right to forget : looking beyond the Google case », *E.J.L.T.*, 2015, Vol. 6, n° 2, pp. 1-25.

- STROWEL A., « Censure ! Vous avez dit censure ? A propos de l'arrêt Google sur le droit à l'oubli », *A&M*, 2014, pp. 311-313.

- STROWEL A., « Le droit à l'oubli : mal nommé, mal défini, mais bienvenu. A propos de l'arrêt Google de la Cour de justice », *in Emile et Ferdinand, Gazette du groupe Larcier*, 2014, n° 7, pp. 4-8.

- SVANTESSON D.J.B., « The Extraterritoriality of EU Data Privacy Law — Its Theoretical Justification and Its Practical Effect on U.S. Businesses », *Stanford Journal of International Law*, 2014, Vol. 50, n° 1, pp. 54-102.

- TAMBOU O., « Arrêt Rynes : la vidéo-surveillance et la directive sur la protection des données personnelles », *J.D.E.*, 2015, pp. 107-108.

- TANKARD C., « What the GDPR means for business », *Network Security*, 2016, n° 6, pp. 5-6.

- TILLINAC J., « Le web 2.0 ou l'avènement du client ouvrier », *Quaderni*, 2006, n° 60, pp. 19-24.

- VAN DER SLOOT B., « Do data protection rules protect the individual and should they ? An assessment of the proposed General Protection Regulation », *International Data Privacy Law*, 2014, pp. 307-325.

- VAN DER SLOOT B., « Welcome to the jungle : de aansprakelijkheid van internetintermediairs voor privacyschendingen in Europa », *Tijdschrif voor Europees en economisch recht*, 2014, pp. 420-431.

- WAKEFIELD J., « Politician and paedophile ask Google to be forgotten », BBC NEWS, 15 mai 2014, http://www.bbc.com/news/technology-27423527 (17 juin 2016).

- WALKER R.K., « The Right to Be Forgotten », *Hastings Law Journal*, 2012, Vol. 64, pp. 257-286.

- WARSO Z., « There's more to it than data protection — Fundamental rights, privacy and the personal/household exemption in the digital age », *Computer Law & Security Review*, 2013, pp. 491-500.

- WEBER R.H., « The Right to Be Forgotten : More Than a Pandora's Box ? », *J.I.P.I.T.E.C.*, 2011, pp. 120-130.

- WEBER R.H., « On the Search for an Adequate Scope of the Right to Be Forgotten », *J.I.P.I.T.E.C.*, 2015, Vol. 6, n° 1, pp. 2-10.

- WHITMAN J.Q., « The Two Western Cultures of Privacy : Dignity Versus Liberty », *The Yale Law Journal*, 2004, Vol. 113, pp. 1151-1221.

- WOODS L., « Big Brother's Little Brother ? The scope of the household exception to EU data protection law », 2014, http://eulawanalysis.blogspot.be/2014/07/big-brothers-little-brother-scope-of.html (17 mars 2016).

- XANTHOULIS N., Conceptualising a Right to Oblivion in the Digital World : A human rights-based approach, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2064503 (13 octobre 2015).

- ZANFIR G., « How CJEU's Privacy Spring constructed the human rights shield in the digital age », 2015, http://www.academia.edu/12458989/How_CJEU_s_Privacy_Spring_construed_the_human_rights_shield_in_the_digital_age (13 février 2016).

- ZANFIR G., « Tracing the Right to Be Forgotten in the Short History of Data Protection Law : The New Clothes of an Old Right », *in Reforming European Data Protection Law* (sous la dir. de S. GUTWIRTH, P. DE HERT et R. LEENES), Dordrecht, Heidelberg, New York, London, Springer, 2015, pp. 227-249.

Avis, rapports et autres

Organes de l'Union européenne

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 1/2008 on data protection issues related to search engines », 4 avril 2008, 00737/EN WP 148.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 5/2009 on online social networking », 12 juin 2009, 01189/09/EN WP 163.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 1/2010 on the concepts of controller and processor », 16 février 2010, 00264/10/EN WP 169.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 2/2010 on online behavioural advertising », 22 juin 2010, 00909/10/EN WP 171. Groupe de travail « Article 29 » sur la protection des données, « Opinion 15/2011 on the definition of consent », 13 juillet 2011, 01197/11/EN WP 187.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 01/2012 on the data protection reform proposals », 23 mars 2012, 00530/12/EN WP 191.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 05/2012 on Cloud Computing », 1er juillet 2012, 01037/12/EN WP 196.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 03/2013 on purpose limitation », 2 avril 2013, 00569/13/EN WP 203.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 01/2014 on the applicable of necessity and proportionality concepts and data protection within the law enforcement sector », 27 février 2014, 536/14/EN WP 211.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC », 9 avril 2014, 844/14/EN WP 217.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 05/2014 on Anonymisation Techniques », 10 avril 2014, 0829/14/EN WP 216.

- Groupe de travail « Article 29 » sur la protection des données, « Guidelines on the implementation of the Court of Justice of the European Union judgement on Google Span and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González C-131/12 », 26 novembre 2014, 14/EN WP 225.

- Groupe de travail « Article 29 » sur la protection des données, « Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing », 22 septembre 2015, 2588/15/EN WP 232.

- Groupe de travail « Article 29 » sur la protection des données, « Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain », 16 décembre 2015, 176/16/EN WP 179 update.

- Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), *C.O.M.* (2003) 265 final.

- 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 donnés à caractère personnel dans l'Union européenne », *C.O.M.* (2010) 609 final.

- Avis du contrôleur européen de la protection des données 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.U.E.*, C 181, du 22 juin 2011, p. 1.

- Avis 2/13 de la Cour (assemblée pléniaire) du 18 décembre 2014 rendu en vertu de l'article 218, paragraphe 11, TFUE, relatif à l'adhésion de l'Union européenne à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Autres

- BACKES M., DRUSCHEL P. et TIRYEA R., Rapport de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) : « The right to be forgotten — between expectations and practice », 2012, https://www.enisa.europa.eu/publications/the-right-to-be-forgotten (13 octobre 2014).

- BOIZARD M., BLANDIN A., CORGAS-BERNARD C., DEDESSUS LE MOUSTIER G. et al., Le droit à l'oubli [Rapport de recherche], Mission de recherche Droit et Justice, 2015, http://www.gip-recherche-justice.fr/publication/le-droit-loubli-2/, (12 octobre 2015).

- COLIN N. et COLLIN P., « Rapport au Minsitre de l'économie et des finances, au Ministre du redresement productif, au Minsitre délégué chargé du budget et à la Ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique — Mission d'expertise sur la fiscalité de l'économie numérique », 2013, http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf (16 mars 2016).

- CYBERLEX (L'association du droit et des nouvelles technologies), « Contribution dans le cadre des travaux sur el droit à l'oubli numérique. L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? », 2010, http://www.cyberlex.org/wp-content/uploads/2015/10/contribution_cyberlex_dao.pdf (13 avril 2016).