

Edouard CRUYSMANS

Assistant à l'Université catholique de Louvain
Chercheur à l'Université Saint-Louis-Bruxelles
Doctorant

Alain STROWEL

Professeur à l'Université catholique de Louvain
et à l'Université Saint-Louis-Bruxelles
Avocat au barreau de Bruxelles

Introduction

1. **Quand le « droit à l'oubli » hante la responsabilité en ligne.** La protection de sa vie privée a toujours été un enjeu important pour la plupart des individus. Cette notion est finalement assez récente, puisqu'elle ne prend réellement son essor qu'à la suite de la Seconde Guerre mondiale. Bien qu'il soit déjà le sujet principal d'un article écrit en 1890 par Samuel Warren et Louis Brandeis¹, le droit à la vie privée se développe en Europe à travers la jurisprudence de la Cour européenne des droits de l'homme étendant la notion, au fil des décisions, à de nouveaux contextes. Depuis quelques années maintenant, faisant face aux développements technologiques et numériques, à l'essor du *big data* et des réseaux sociaux, une nouvelle composante du droit au respect de la vie privée se façonne au gré de décisions jurisprudentielles. La présente contribution a vocation à mettre en lumière, à partir de ces cas concrets, la consécration de ces nouvelles prérogatives juridiques que l'on peut regrouper sous l'appellation générique de « droit à l'oubli ». Ce « droit » doit faire face à la persistance de la mémoire numérique qui nous fait craindre « une mise à nu », sans espoir que nos données puissent un jour tomber dans les pénombres de l'oubli². L'on ne peut évidemment nier ces craintes tant elles sont légitimement fondées. Cela étant, comme le souligne Mélanie Clément-Fontaine, il y a lieu de relativiser en partie ce mythe de la mémoire absolue dès lors que cette capacité numérique demeure fragile : « [u]ne fragilité tout d'abord technique puisque les supports ou les formats ne sont pas aussi pérennes que le papier ; ensuite une fragilité des données, dont la manipulation [...] est plus aisée et parfois moins visible »³. À ces deux fragilités, nous pouvons en ajouter une troi-

¹ S. D. WARREN et L. D. BRANDEIS, « The right to privacy », *Harvard Law Review*, 1890, pp. 193-220.

² M. CLÉMENT-FONTAINE, « Faut-il se réjouir de la percée du droit à l'oubli numérique ? », note sous Cass., 29 avril 2016, et Cass. fr. (1^{re} ch. civ.), 12 mai 2016, *A.M.*, 2016/5-6, p. 454.
³ *Ibid.*

sième : la mémoire numérique est encore affaiblie face à la quantité des données stockées, aboutissant *de facto* à diluer les informations dans la masse et à réduire, comme dans d'autres cas d'inflation, la valeur des unités (ici d'information).

Cela étant, les juges sont de plus en plus souvent amenés à se pencher sur des problématiques liées à la permanence des données sur Internet. De nouveaux instruments juridiques sont développés et, dans les textes juridiques, il est question d'oubli, d'anonymisation, de retrait, de suppression, d'effacement, de déréfèrement, d'opposition, de rectification, etc. Certaines de ces prérogatives sont assez récentes, d'autres sont plus anciennes. Certaines sont d'ores et déjà formalisées dans des textes législatifs, d'autres sont issues de raisonnements jurisprudentiels. Ces droits se rejoignent en ce qu'ils se traduisent, sur le plan judiciaire, en des actions en responsabilité pour atteinte au droit à la vie privée et/ou au droit au respect des données à caractère personnel. Sur le plan des catégories juridiques, ces droits s'inscrivent tous dans ce que l'on nomme communément le « droit à l'oubli » ou le « droit à l'oubli numérique », tel qu'il est notamment repris dans le Règlement général européen sur la protection des données n° 2016/679 entré en application depuis le 25 mai 2018 (ci-après, le « RGPD » ou le « règlement »)⁴.

Principalement, la présente contribution s'attarde sur deux droits. Premièrement, le droit au déréfèrement (section 1) consacré dans l'arrêt *Google Spain*⁵ par application des dispositions relatives à la protection des données

⁴ Règlement 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 95/46/CE (Règlement général sur la protection des données), J.O.U.E., L119 du 4 mai 2016. Le règlement est entré en vigueur le 25 mai 2016, mais il s'applique depuis le 25 mai 2018 (art. 99 du règlement).

⁵ C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12, A.M., 2014/5, p. 398, note J. AUSLOOS et B. VAN ALSENOY, « Bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens » ; Computerr, 2014, p. 226, note P. VAN ECKE et A. CORNETTE, « De verantwoordelijkheid van zoekmachines bij de publicatie van persoonsgegevens op websites: Het Google Spain SL arrest » ; *Juristenkrant*, 2014/290, p. 2 (reflet); J.D.E., 2014, p. 271; J.T., 2014, p. 451, note E. CRUYSMANS et A. STROWEL, « 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.L.M.B., 2014, note A. CASSART et J. HENROTTE, « Arrêt Google Spain : la révélation d'un droit à l'effacement plutôt que la création d'un droit à l'oubli » ; R.E.D.C., 2014, p. 53; R.W., 2014-2015, p. 997; S.E.W., 2014, p. 344 (reflet); R.D.C., 2014, p. 724.

Voy. encore d'autres commentaires de cet arrêt : C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréfèrement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », in A. GROSJEAN (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, coll. Création Information Communication, Bruxelles, Larcier, 2015, pp. 237-268; M. AUBERT, E. BOUSSY et H. CASSAGNABERE, « Chronique de jurisprudence de la C.J.U.E. Vie privée et protection des données personnelles – Moteurs de recherche et droit à l'oubli », A.J.D.A., 2014/20, pp. 1147-1149; C. BERNARD-GLANZ, « Les arrêts *Digital Rights Ireland* et *Google Spain*, ou le printemps européen de la protection des données », C.D.E., 2014/3, pp. 685-717; D. LINDSAY, « The "Right to be forgotten" by search engines under data privacy law: A legal analysis of the Costeja ruling », *Journal of Media Law*, 2014/6, pp. 159-179; E. DEFREYNE et R. ROBERT, « L'arrêt "Google Spain" : une clarification de la responsabilité des

personnelles de la directive 95/46/CE, laquelle a depuis peu cédé sa place au règlement susmentionné. Quant au droit à l'anonymisation développé dans la seconde section, il autorise la suppression d'informations figurant notamment dans les archives des journaux. Il s'agit là de deux droits devant être revendiqués auprès de personnes distinctes : le déréfèrement se demande auprès de l'exploitant d'un moteur de recherche, l'anonymisation auprès d'un responsable de site Web⁶.

Section 1

Le droit au déréfèrement

Sous-section 1

Qu'est-ce que le droit au déréfèrement ?

2. **Oubli et droit au déréfèrement.** Il y a lieu de distinguer ce qui est communément appelé « le droit à l'oubli » et le droit au déréfèrement. Le droit au déréfèrement constitue une façon, parmi d'autres, d'obtenir la suppression d'informations ou de données. En ce sens, il se conçoit comme une forme de limitation de la liberté de diffuser et de recevoir l'information. Aujourd'hui, notamment avec le développement des règles relatives au traitement des données personnelles, cette limitation se traduit dans diverses prérogatives, dont le droit au déréfèrement ou le droit à l'anonymisation (voy. *infra*, n°s 28 et s.). Ce constat avait déjà été fait par les membres du Comité consultatif réuni par Google pour analyser la mise en œuvre de l'arrêt *Google Spain* de la Cour de justice de l'Union européenne. Dans son rapport, le Comité soulignait que « [t]he Ruling has been widely referred to as creating a "Right to be Forgotten". [...] In fact, the Ruling does not establish a general Right to be Forgotten. Implementation of the Ruling does not have the effect of "forgetting" information about a data subject. Instead, it requires Google to remove links [...] Throughout this report, we shall refer to the process of removing links in search results based on queries for an individual's name as "delisting". Once delisted, the information is still available at the source site, but its accessibility to the general public is reduced because search queries against the data subject's name will not return a link to the source publication »⁷.

moteurs de recherche... aux conséquences encore floues », R.D.T., 2014/3, pp. 73-114; O. LINKSEY, « Control over personal data in a digital age: Google Spain v. AEPD and Mario Costeja González », *The Modern Law Review*, 2015/78(3), pp. 522-534; P. VAN DEN BULCK, « Arrêt Google Spain : l'étendue du droit à l'oubli », J.D.E., 2014, pp. 289-290; G. VOSS, « The right to be forgotten in the European Union : enforcement in the Court of Justice and amendment to the proposed general data protection regulation », *Journal of Internet Law*, 2014/18, pp. 3-8; J.-P. FOEGLE, « La C.J.U.E. magicienne européenne du "droit à l'oubli" numérique », *Rev. dr. h.*, mis en ligne le 16 juin 2014, [www.http://revdh.revues.org/840](http://revdh.revues.org/840).

⁶ Quoiqu'un déréfèrement puisse aussi être exigé de la part de l'éditeur d'un site Web ayant un moteur de recherche interne, comme c'est souvent le cas des éditeurs de presse. Cela étant, l'impact d'une telle demande demeure limité.

⁷ The Advisory Council to Google on the Right to be Forgotten, 6 février 2015, pp. 3-4.

3. Définir le déréférencement. Le déréférencement est défini par le dictionnaire *Le Larousse* comme étant une « [o]pération par laquelle un distributeur supprime un produit des références qu'il commercialise ». La définition proposée nous semble axée essentiellement dans une dimension commerciale et de marketing. Pourtant, dans l'acception qui nous importe dans le cadre de cette contribution, le déréférencement s'écarte de ces domaines d'application – bien que des comparaisons puissent éventuellement être faites. Aussi, faut-il davantage entendre le déréférencement comme étant « le procédé selon lequel les liens vers certains contenus écrits/audios/vidéo/photo graphiques disponibles sur [l]Internet (le "contenu") sont supprimés, des résultats générés par les fournisseurs de services de moteurs de recherche, après que des mots-clés précis [ont] été insérés dans l'outil de barre de recherche de ces mêmes moteurs de recherche »⁸.

La Commission nationale française de l'informatique et des libertés, la CNIL, indique, sur son site Internet, que le « droit au déréférencement vous permet de demander à un moteur de recherche de supprimer certains résultats de recherche associés à vos noms et prénoms. Il consiste à supprimer l'association d'un résultat de votre nom et votre prénom. Cette suppression ne signifie pas l'effacement de l'information sur le site Internet source. Le contenu original reste ainsi inchangé et est toujours accessible via les moteurs de recherche en utilisant d'autres mots-clés de recherche ou en allant directement sur le site à l'origine de la diffusion »⁹.

Il est intéressant de souligner que le déréférencement constitue un mode de réparation, au même titre que l'anonymisation d'informations dont il sera question dans le second chapitre.

Sous-section 2

La consécration du droit au déréférencement

A. La consécration dans l'arrêt *Google Spain*: analyse des dispositions de la directive 95/46/CE

4. *Google Spain*, ou la consécration du droit au déréférencement ? La présente contribution nous offre l'opportunité de nous pencher à nouveau sur l'arrêt rendu par la Cour de justice de l'Union européenne le 13 mai 2014, dans l'affaire *Google Spain*. L'objectif n'est pas de proposer un énième commentaire d'un arrêt qui a lui-même été déjà abondamment commenté¹⁰. Cela étant, se replonger dans le raisonnement juridique suivi par les juges européens afin

⁸ A. GAUBERT, « Comment obtenir le déréférencement sur Google ? », www.lesechos.fr, mis en ligne le 21 novembre 2017, consulté le 19 mars 2018.

⁹ www.cnil.fr.

¹⁰ Nous renvoyons aux commentaires listés à la note 5 de la présente contribution.

de répondre aux questions préjudicielles posées nous permet de clarifier – et nous estimons qu'en matière d'oubli et de droit au déréférencement, cela s'avère nécessaire – la démarche qui a permis à la Cour de consacrer ce déréférencement. En outre, une telle approche nous permet aussi de confronter les développements fondés sur la directive 95/46/CE aux dispositions du Règlement général sur la protection des données, désormais d'application.

Dans un premier temps, on le sait, la Cour a reconnu que l'exploitant d'un moteur de recherche tel que Google « collecte » des données personnelles 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 de résultats de leurs recherches » (§ 28 de l'arrêt). L'ensemble de ces opérations constitue, selon les termes de l'article 2, b), de la directive, un traitement¹¹, « sans qu'il importe que l'exploitant du moteur de recherche applique les mêmes opérations également à d'autres types d'information et ne distingue pas entre celles-ci et les données à caractère personnel » (§ 28). La Cour ajoute que l'exploitant du moteur de recherche est le « responsable du traitement »¹² dès lors qu'il détermine les finalités et les moyens du traitement. Elle rejette en ce sens l'argumentation tenue par l'avocat général qui soutenait qu'un fournisseur de services de moteur de recherche ne pouvait être considéré comme responsable qu'à la condition qu'il puisse opérer un contrôle sur les données à caractère personnel¹³, ce qui, *in casu*, n'est pas le cas, puisque Google ne fait que traiter des données diffusées licitement par divers sites Web.

Ensuite, dans la deuxième question préjudicielle posée à la Cour de justice, cette dernière s'interroge sur le débiteur de cette éventuelle obligation de suppression d'information qui, à ce stade de l'arrêt, n'est pas encore consacrée. En d'autres termes, est-il possible de s'adresser à l'exploitant d'un moteur de recherche afin de supprimer des liens d'une liste de résultats alors même que

¹¹ Dans le règlement n° 2016/679, l'esprit de la définition du terme « traitement » demeure le même que celui de la directive 95/46/CE. Cela étant, quelques minimales modifications ont été apportées. L'article 4, 2), du règlement le définit comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, [tels] la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction » (les modifications apparaissent en italique).

¹² L'article 2, d), de la directive se retrouve en grande partie à l'article 4, 7), du règlement. Ce dernier définit le responsable de traitement comme étant « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre » (les modifications apparaissent en italique).

¹³ Concl. Av. gén. M. Niiilo Jääskinen du 25 juin 2013, *Google Spain* St. Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, §§ 84-90.

les informations litigieuses sont encore disponibles sur le « site source » et, le cas échéant, alors même que leur diffusion est tout à fait licite ? La Cour de justice y entrevoit en réalité deux sous-questions auxquelles elle s'attelle à répondre : d'une part, l'obligation de suppression d'information, et, d'autre part, la scission potentielle des responsabilités des deux types d'intermédiaires cités ci-avant.

Premièrement, elle s'interroge sur l'existence d'une obligation de suppression de données litigieuses. L'article 12, b), de la directive qui consacre le droit d'obtenir la rectification, l'effacement ou le verrouillage est susceptible de s'appliquer dès lors que les conditions relatives à la qualité des données (art. 6 de la directive) et les principes propres à la légitimité du traitement (art. 7 de la directive) ne sont pas respectés. Il importe de souligner qu'en l'espèce – mais une généralisation doit être envisagée pour l'ensemble des moteurs de recherche –, le traitement effectué par l'exploitant du moteur de recherche relève de l'article 7, f), de la directive, ce dernier énonçant que le traitement est légitime s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée [...]. La Cour souligne que l'application de cette disposition « nécessite ainsi une pondération des droits et des intérêts opposés en cause dans le cadre de laquelle il doit être tenu compte de l'importance des droits de la personne concernée » (§ 74). Pour la Cour, le droit d'opposition consacré par l'article 14 de la directive peut, en outre, être invoqué. Ce cumul est plausible d'autant plus que l'opposition peut être revendiquée « au moins dans les cas visés à l'article 7, points e) et f), [...] à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière [...] » (art. 14, al. 1^{er} a)). En d'autres termes, l'application de cet article implique, elle aussi, une pondération des intérêts en présence : les intérêts du responsable du traitement doivent être mis en balance avec les intérêts de la personne concernée.

Il est intéressant de souligner la prise en compte de cet équilibre, alors qu'on eût pu croire que l'application de la réglementation relative aux données personnelles avait un effet plus automatique. Il n'en est rien. La Cour poursuit d'ailleurs son raisonnement en évoquant quelques critères permettant d'effectuer cette balance des intérêts, critères qu'elle qualifie de « conditions d'application des articles 12, sous b), et 14, premier alinéa, sous a) » (§ 82). Ainsi, le seul intérêt économique de l'exploitant d'un moteur de recherche ne peut justifier une telle ingérence dans les droits consacrés par les articles 7 (respect de la vie privée et familiale) et 8 (protection des données à caractère personnel) de la Charte des droits fondamentaux de l'Union européenne. Cela étant, si, à cet intérêt économique, s'ajoute « l'intérêt légitime des internautes potentiellement intéressés à avoir accès » (§ 81) aux données, il y a alors lieu de rechercher ce juste équilibre. En l'espèce, dans le cadre des fonctions d'un moteur de recherche, ce second intérêt nous semble toujours présent, de sorte qu'il nous

paraît difficile de ne pas effectuer cette recherche. Dans cette perspective, les juges européens indiquent que, « [s]i, certes, les droits de la personne concernée protégés par ces articles prévalent également, en règle générale, sur ledit intérêt des internautes, cet équilibre peut toutefois dépendre, dans des cas particuliers », d'une série de critères proposés. L'enseignement nous semble important : pour la Cour, la règle veut que la protection de la vie privée et des données à caractère personnel de la personne concernée prévale sur l'intérêt des internautes. Alors que l'adverbe « également » renvoie à la hiérarchisation faite entre le seul intérêt économique et les droits de la personne concernée, la Cour prend cependant quelques précautions stylistiques, soutenant que ce nouvel ordonnancement existe « en règle générale » et que l'équilibre dépend « toutefois » de certaines circonstances. Et de conclure sur cette première sous-question que l'autorité judiciaire saisie ou l'autorité de contrôle des données peut « ordonner audit exploitant de supprimer de la liste des résultats » des liens, alors même que les données sont accessibles sur le site source¹⁴. Autrement dit, les articles 12, b), et 14, alinéa 1^{er} a), dans leur application concrète à l'égard d'un exploitant de moteur de recherche, aboutissent à requérir la suppression de liens, c'est-à-dire, pratiquement, le déréférencement. Cette conclusion est d'ailleurs confirmée dans les lignes directrices du Groupe de travail « Article 29 » relatives à l'implémentation de l'arrêt *Google Spain*¹⁵.

Deuxièmement, l'autre sous-question soulevée est celle de la distinction des responsabilités de l'exploitant du moteur de recherche et de l'éditeur d'une page Web. Tous deux effectuent des traitements de données qui affectent les droits fondamentaux de la personne concernée (§ 83). Pour la Cour, le traitement effectué par l'exploitant d'un moteur de recherche « est susceptible de constituer une ingérence plus importante dans le droit fondamental au respect de la vie privée » (§ 87), dès lors que l'accessibilité à l'information en est grandement facilitée. A propos de la responsabilité de l'éditeur, la Cour met cependant en garde, compte tenu de l'existence, à l'article 9 de la directive, de dérogations pour les traitements effectués « aux seules fins de journalisme ». En effet, dès lors qu'un traitement est justifié par une telle finalité, la revendication et l'application des droits visés aux articles 12, b), et 14, alinéa 1^{er} a), sont exclues à l'égard de l'éditeur d'une page Web (§ 85). A demi-mot¹⁶, la Cour paraît

¹⁴ Voy, en ce sens, le paragraphe 84 de l'arrêt : « [à] cet égard, il y a lieu de relever que, compte tenu de la facilité avec laquelle des informations publiées sur un site Web peuvent être répliquées sur d'autres sites et du fait que les responsables de leur publication ne sont pas toujours soumis à la législation de l'Union, une protection efficace et complète des personnes concernées ne pourrait être réalisée si celles-ci devaient d'abord ou en parallèle obtenir l'effacement des informations les concernant auprès des éditeurs de sites Web ».

¹⁵ Art. 29 Data Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union judgement on « Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González »* C-131/12, document WP 225, 26 novembre 2014.

¹⁶ Voy. l'arrêt qui précise que « le traitement par l'éditeur d'une page Web, consistant dans la publication d'informations relatives à une personne physique, peut, le cas échéant, être effectué » aux seules fins de

considérer qu'un traitement effectué par un exploitant d'un moteur de recherche dans le cadre d'une requête effectuée en ligne par un internaute n'est pas un traitement effectué « aux seules fins de journalisme ». Nous abondons dans le sens de la Cour en estimant que l'intérêt économique non négligeable semble être la justification déterminante d'un tel traitement. Enfin, dans les cas où ladite dérogation n'est pas d'application¹⁷, et dans l'hypothèse où les traitements seraient justifiés par le motif visé à l'article 7, f)¹⁸, la mise en balance des intérêts peut diverger selon qu'elle est effectuée à l'encontre de l'exploitant du moteur de recherche ou à l'encontre de l'éditeur d'une page Web (§ 86).

Quant à la troisième question préjudicielle, elle concerne la suppression de données à caractère personnel justifiée par le fait que ces dernières portent préjudice à ladite personne concernée ou que celle-ci souhaite tout simplement que les informations litigieuses soient oubliées. La requête s'appuie sur les mêmes dispositions, soit les articles 12, b), et 14, alinéa 1^{er}, a), de la directive. Selon la Cour, il faut déduire des exigences relatives à la qualité des données (art. 6 de la directive) « que même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées » (§ 93). Les juges européens ajoutent que « [t]el est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé » (§ 93). Cet examen de l'inadéquation, de l'absence de pertinence ou de l'excessive s'opère « eu égard à l'ensemble des circonstances caractérisant le cas d'espèce » (§ 94). A nouveau, la Cour semble exiger la réalisation d'une balance des intérêts en présence. Elle écrit d'ailleurs qu'« il convient notamment d'examiner si la personne concernée a un droit à ce que l'information relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats, affichée à la suite d'une recherche effectuée à partir de son nom. À cet égard, il convient de souligner que la constatation d'un tel droit ne présuppose pas que l'inclusion de l'information en question dans la liste de résultats cause un préjudice à la personne concernée » (§ 96). Autrement dit, le

journalisme" et ainsi bénéficier, en vertu de l'article 9 de la directive 95/46, de dérogations aux exigences établies par celle-ci, tandis que tel n'apparaît pas être le cas s'agissant du traitement effectué par l'exploitant d'un moteur de recherche » (nous soulignons). La formule n'est pas totalement précise.

La Cour, en effet, ne généralise pas cette application dès lors qu'on est en présence d'une requête à l'encontre d'un éditeur de pages Web. En son paragraphe 85, la Cour, prudente, indique que « le traitement par l'éditeur d'une page Web, consistant dans la publication d'informations relatives à une personne physique, peut, le cas échéant, être effectué "aux seules fins de journalisme" et ainsi bénéficier, en vertu de l'article 9 de la directive 95/46, de dérogations aux exigences établies par celle-ci, tandis que tel n'apparaît pas être le cas s'agissant du traitement effectué par l'exploitant d'un moteur de recherche » (nous soulignons).

La Cour souligne cependant que ces motifs pourraient diverger. Cela étant, le droit d'opposition visé à l'article 14, alinéa 1^{er}, a), de la directive est susceptible de s'appliquer selon la directive « au moins dans les cas visés à l'article 7, points e) et f) » (nous soulignons).

droit à voir des données supprimées ou oubliées est indépendant de l'existence d'un préjudice particulier.

Le constat est clair : dans les deux réponses apportées par la Cour aux deux dernières questions préjudicielles posées, les juges européens requièrent qu'un équilibre soit recherché en se basant sur les intérêts en présence. Comment pratiquement exécuter celui-ci et sur la base de quels critères ? Nous l'avons déjà en partie abordé en relatant la réponse apportée par la Cour à la deuxième question. Cela étant, les juges européens ajoutent quelques précieuses informations dans le cadre de la troisième question préjudicielle. Rétirant sa hiérarchisation des droits (« il y a lieu de considérer [...] que [les droits consacrés aux articles 7 et 8 de la Charte] prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à trouver ladite information lors d'une recherche »¹⁹), la Cour permet que cette présomption de prévalence soit renversée pour autant que l'on applique de manière stricte certains critères. Ainsi, il y a lieu de prendre en compte le rôle joué par la personne concernée dans la vie publique, l'existence d'un intérêt prépondérant du public à avoir accès à l'information, ainsi que la sensibilité de l'information et le laps de temps écoulé entre la publication initiale et la nouvelle divulgation faite dans la liste des résultats du moteur de recherche. La plupart de ces critères correspondent aux facteurs de pondération retenus par la Cour européenne des droits de l'homme dans la résolution des conflits entre le droit à la liberté d'expression et le droit à la protection de la vie privée²⁰. Compte tenu de la mise en pratique de ces indices, l'application des articles 12, b), et 14, alinéa 1^{er}, a), à l'égard d'un exploitant de moteur de recherche peut exiger de sa part qu'il supprime des liens d'une liste de résultats.

B. Le déréférencement dans le RGPD : comparaison des dispositions de la directive 95/46/CE et du RGPD

5. Un cas *Google Spain* sous le RGPD. Si l'on devait, demain, appliquer le RGPD aux faits de l'affaire *Google Spain*, on aboutirait au même résultat, même si les dispositions invoquées diffèrent, notamment parce que les droits des personnes sont davantage explicités et développés dans le RGPD. Les prérogatives consacrées dans les articles 12, b), et 14, alinéa 1^{er}, a), de la directive se retrouvent en réalité dans plusieurs dispositions du règlement, à savoir les articles 16, 17, 18 et 21.

¹⁹ Voy. le paragraphe 97, celui-ci renvoyant d'ailleurs au paragraphe 81, là où la Cour a déjà tenu ce raisonnement. Nous renvoyons à notre brève analyse faite ci-avant.

²⁰ Voy., p. ex., Cour eur. D.H. (gde ch.), 7 février 2012, *von Hannover c. Allemagne* (n° 2), req. 40660/08 et 60641/08 ; Cour eur. D.H. (gde ch.), 7 février 2012, *Axel Springer c. Allemagne*, req. 39954/08.

6. Le contenu de l'article 16. L'article 16 évoque le droit de rectification. Il énonce que « [l]a personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire ».

L'on note d'emblée que la disposition semble plus restrictive en ce qu'elle ne vise que les données inexactes, sans effectuer un renvoi exemplatif comme le faisait la disposition de la directive. L'article 16 consacrant ce droit de rectification est, en effet, à lire en parallèle avec l'article 5, § 1^{er}, d), du règlement²¹ qui précise que les données doivent être « exactes et, si nécessaire, tenues à jour », ajoutant que « toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ».

Outre le droit de rectification, l'article 16 semble consacrer un second droit permettant de compléter des informations considérées comme étant incomplètes par la personne concernée « compte tenu des finalités du traitement ».

En guise de conclusion de cette brève analyse de l'article 16, et eu égard au prisme de cette contribution, nous considérons qu'une application de l'article 16 du règlement ne permet pas d'obtenir le déréférencement de liens. Tel n'est, à notre estime, pas son objectif, d'autant plus que les droits consacrés semblent pouvoir être invoqués à l'égard de l'éditeur d'une page Web, et non à l'égard d'un exploitant de moteur de recherche.

2. L'article 17 – Le droit à l'effacement²²

7. Oubli ou effacement? L'article 17 du règlement évoque le droit à l'oubli numérique, sans toutefois le consacrer clairement. En effet, il suffit de prendre en compte les réserves de forme avec lesquelles ce droit figure dans le règlement : premièrement, l'article s'intitule bien « Droit à l'effacement », l'appellation « droit à l'oubli » ne semblant être que secondaire ; deuxièmement, les rédacteurs du règlement ont pris soin de recourir à l'utilisation de guillemets ainsi que de parenthèses. Cela témoigne, sans aucun doute, de la timidité avec laquelle le législateur européen consacre cette prérogative²³. Et cela traduit, sans

nul doute, les débats intenses qui ont entouré cet article, tant les enjeux relatifs à la protection de la vie privée que les enjeux économiques étaient importants. Enfin, il est intéressant de remarquer que l'expression « droit à l'oubli » n'est jamais reprise dans le contenu de l'article 17, voire même dans le contenu d'aucun autre article du règlement²⁴. Ces éléments nous permettent, par conséquent, de douter de la consécration d'un réel droit à l'oubli numérique dans ce règlement européen. Tout au plus, l'objectif d'oubli trouve son fondement à travers d'autres prérogatives qui, pour la plupart, figuraient déjà dans le texte de la directive européenne. L'article 17 qui organise le droit à l'effacement en est l'exemple le plus clair.

L'article 17 développe considérablement le droit à l'effacement tel qu'il était prévu à l'article 12 de la directive 95/46/CE. En effet, l'article 12, b), évoquait l'effacement possible lorsque les données n'étaient pas conformes aux principes relatifs à la qualité des données (art. 6 de la directive) et à la légitimation des traitements (art. 7 de la directive). Dans le règlement, le droit à l'effacement permet d'obtenir, « dans les meilleurs délais », l'effacement de données à caractère personnel dans six situations (art. 17, § 1^{er}) : l'absence de nécessité des données au regard des finalités du traitement, le retrait du consentement de la personne concernée, l'exercice d'un droit d'opposition, l'illicéité du traitement, l'imposition de l'effacement par une obligation légale, ou lorsque les données sont collectées pour des services de la société de l'information à destination des enfants. Ce droit implique l'obligation, pour le responsable du traitement, d'effacer ces données « dans les meilleurs délais »²⁵. L'article 17, § 2, innove au regard de la directive en ce qu'il prévoit, pour le responsable de traitement qui a rendu publiques des données personnelles, une obligation de prendre des mesures – en ce compris des mesures techniques – pour avertir l'ensemble des autres responsables de traitement de l'existence d'une demande d'effacement. Cette obligation est atténuée dès lors qu'elle existe « compte tenu des technologies disponibles et des coûts de mises en œuvre »²⁶. Elle a vocation à augmenter l'impact de la demande d'effacement formulée par la personne concernée et à limiter, en partie au moins, les effets ubiquitaires d'Internet en évitant à la personne concernée de multiplier les demandes d'effacement auprès de chaque responsable de traitement. Toutefois, la disposition reconnaît elle-même les limites de ce procédé. Les conditions de mise en œuvre de cette obligation demeurent floues dès lors qu'elle n'est imposée que dans la mesure du raisonnable. Mais qu'est-ce qui est raisonnable ? Quelques

²¹ Voy. aussi le considérant 59 du règlement.

²² Les développements proposés relatifs à l'article 17 sont en partie tirés de la contribution suivante : E. CRUYSMANS, « La protection de la réputation en ligne : droit de réponse, droit de rectification, droit à l'oubli », in C. DE TERWAGNE et Q. VAN ENIS (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2018, à paraître.

²³ Voy. cependant M. CLÉMENT-FONTAINE, « Faut-il se réjouir de la percée du droit à l'oubli numérique ? », *op. cit.*, p. 454. L'auteur écrit, dans sa note 14, ceci : « [q]u'il importe le titre : l'effacement, c'est l'oubli ».

²⁴ Voy. toutefois, les considérants 65 et 66 qui reprennent l'expression « droit à l'oubli numérique ».

²⁵ La redondance de l'expression « dans les meilleurs délais » s'expliquerait par la dissociation de deux étapes dans l'exercice de ce droit, la première permettant d'obtenir l'effacement (validation de principe), la seconde impliquant concrètement l'effacement (exécution).

²⁶ L'atténuation prend en compte les difficultés inhérentes au réseau Internet et à l'impossibilité concrète d'être en connaissance de tous les autres traitements effectués par d'autres responsables sur les mêmes données. Elle nous semble, par conséquent, cohérente, permettant d'assurer une certaine efficacité à cette nouvelle obligation. En cela, l'obligation d'information semble constituer une obligation de moyens.

balises seront nécessaires pour le préciser, tant à l'attention des responsables de traitement que des personnes concernées.

Quant au dernier paragraphe de l'article 17, il prévoit une série d'exceptions : il n'y a pas d'effacement dans la mesure où le traitement est nécessaire à la liberté d'expression ou d'information, lorsqu'une obligation légale doit être respectée, lorsque des motifs de santé publique l'exigent, lorsque le traitement est justifié par des fins archivistiques, scientifiques, historiques ou statistiques, et, enfin, lorsqu'un traitement est nécessaire à la constatation, l'exercice ou la défense de droits en justice. L'application de ces exceptions revient à requérir, de la part du responsable du traitement, qu'il effectue une pondération des intérêts en présence. Très certainement, la première exception se révélera complexe à mettre en œuvre. Elle renvoie en réalité à l'article 85 du règlement qui énonce que les « États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement 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 » (§ 1^{er}). Le paragraphe 2 de cette même disposition énonce encore que les traitements réalisés à des fins journalistiques permettront aux États membres d'adopter des exemptions ou dérogations notamment aux droits de la personne concernée. Ces exceptions doivent cependant être justifiées par la nécessaire conciliation du droit à la protection des données à caractère personnel et du droit à la liberté d'expression et d'information (art. 85, § 2, *in fine*). Ce régime qui laisse une marge de manœuvre aux États membres semble quelque peu contredire l'uniformisation renforcée liée à l'usage d'un règlement plutôt que d'une directive.

L'article 17 du règlement ne permet pas le déréfèrencement. La disposition prévoit l'effacement, un recours basé sur cet article devant être actionné contre l'éditeur d'un site Web, et non contre l'exploitant d'un moteur de recherche.

3. L'article 18 – Le droit à la limitation

8. Le contenu de l'article 18. L'article 18 consacre la limitation du traitement des données²⁷. La limitation des données fait l'objet d'une définition dans le règlement : il s'agit du « marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur » (art. 4, 3), du règlement). Concrètement, le considérant 67 souligne que « [l]es méthodes visant à limiter le traitement de données à caractère personnel pourraient consister, entre autres, à déplacer temporairement les données sélectionnées vers un autre système de traitement, à rendre les données à caractère personnel sélectionnées inaccessibles aux utilisateurs, ou à retirer temporairement les données publiées d'un

²⁷ Ce droit n'était pas présent dans la proposition initiale du règlement. Il apparaît dans la seconde proposition de règlement qui date du 11 juin 2015.

site Internet. Dans les fichiers automatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques de façon à ce que les données à caractère personnel ne fassent pas l'objet d'opérations de traitements ultérieures et ne puissent pas être modifiées. Le fait que le traitement des données à caractère personnel est limité devrait être indiqué de manière claire dans le fichier». Le déréfèrencement pourrait-il être considéré comme une méthode visant à limiter le traitement des données ? À lire le considérant, rien ne semble s'y opposer, le déréfèrencement pouvant notamment se faire temporairement.

Plusieurs cas de limitation sont énumérés dans le paragraphe 1^{er}.

– Ainsi, le point a) permet de limiter le traitement lorsque « l'exactitude des données à caractère personnel est contestée par la personne concernée », cette limitation étant cependant temporaire puisqu'elle opère « pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ». À lire l'article, dès lors que la vérification est faite, la limitation prend fin. Autrement dit, revendiquer son droit à la limitation du traitement n'est efficace qu'à partir du moment où, en parallèle, une action en rectification est introduite dans l'hypothèse où les données s'avèreraient non exactes.

– Le point b) permet de limiter un traitement lorsque celui-ci est « illicite et [que] la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ». Les exigences semblent être ici cumulatives, la limitation n'intervenant qu'après démonstration de l'illégalité des informations et l'exercice de son droit d'opposition consacré à l'article 21 du règlement. En outre, il n'est fait aucune mention du caractère permanent ou temporaire de la mesure, la limitation permanente s'apparentant, en réalité, à la suppression des données personnelles litigieuses.

– Le point c) évoque une limitation lorsque « le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement, mais [que] celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ». La possibilité de limiter le traitement semble, dans ce cas, être en faveur de la personne concernée.

– Enfin, le point d) organise la limitation du traitement lorsque « la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1^{er}, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée ».

Les paragraphes 2 et 3 énoncent des principes applicables à partir du moment où la limitation est admise dès lors que l'on se trouve dans une des hypothèses visées au paragraphe 1^{er}. L'objectif est de restreindre un nouveau traitement de données dont le traitement initial aurait été limité (§ 2) ainsi que d'obliger le

responsable de traitement à informer la personne concernée lors de la levée de la limitation, lorsque cette mesure n'est que temporaire.

9. Comparaison avec la directive. L'article 18, § 1^{er}, a), est la seule hypothèse tirée de l'article 12, b), de la directive. Les trois autres cas ne semblent pas évoqués dans l'ancien texte. En outre, la portée de l'article 18, § 1^{er}, a), nous paraît considérablement limitée au regard de la disposition de la directive. En effet, l'article 12, b), avait une portée plus large dès lors qu'il évoquait la non-conformité d'un traitement, « notamment en raison du caractère incomplet ou inexact des données ». La disposition renvoyait effectivement à l'ensemble des principes relatifs à la qualité des données (art. 6 de la directive) et à la légitimité du traitement (art. 7 de la directive). Tel ne semble plus être le cas : l'article 18, § 1^{er}, a), du règlement ne s'applique qu'en cas de non-respect du principe d'exactitude mentionné à l'article 5, § 1^{er}, d), du règlement.

4. L'article 21 – Le droit d'opposition

10. Le contenu de l'article 21. Le contenu de l'article 14, alinéa 1^{er}, a), de la directive trouve désormais sa place à l'article 21, § 1^{er}, du règlement. Ce dernier est rédigé comme suit : « [l]a personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice ». L'article 6, § 1^{er}, f), précise qu'un traitement est licite lorsqu'il « est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ».

Dans le cas de l'affaire *Google Spain* (voy. *supra*, n° 4), les revendications de suppression d'informations soutenues sur le fondement d'une application des articles 12, b), et 14, alinéa 1^{er}, a), de la directive ont abouti à l'exécution d'une balance des intérêts dès lors que les deux dispositions citées devaient se lire parallèlement à l'article 7, f), auquel elles renvoyaient plus ou moins clairement²⁸. En l'espèce, l'article 21, afin d'être mis en œuvre, renvoie, lui aussi, à cette même disposition. Ceci nous permet dès lors de suivre le même raisonnement que celui tenu par la Cour de justice de l'Union européenne : le droit d'opposition peut être revendiqué à l'égard d'un exploitant de moteur de

²⁸ Pour l'article 14, le renvoi est clair. En revanche, il l'est moins pour l'article 12, b). Ce n'est que parce que la Cour a considéré que cette disposition renvoyait en fait aux principes de qualité des données et de légitimité des traitements que ce renvoi vers la finalité mentionnée à l'article 7, f), est envisageable.

recherche, celui-ci effectuant un traitement nécessaire aux fins de ses intérêts légitimes, afin d'obtenir le déréférencement de liens. Cela étant, une balance des intérêts doit être effectuée, prenant en compte la hiérarchisation faite par la Cour ainsi que les critères d'application proposés par cette dernière.

5. L'article 85 – Les exceptions en faveur de la liberté d'expression

11. Le contenu de l'article 85. Comme évoqué dans le cadre de l'analyse de l'article 17 du règlement (voy. *supra*, n° 7), l'article 85 permet aux États membres d'adopter des dispositions afin de concilier la protection des données à caractère personnel et la liberté d'expression et d'information, en ce compris le traitement effectué à des fins journalistiques. L'article 85, § 2, liste les chapitres du règlement pour lesquels des dérogations en faveur du traitement à des fins de journalisme doivent être prévues. De telles exemptions étaient d'ores et déjà prévues dans le texte de la directive, à l'article 9. Cela étant, l'article 85 nous paraît être plus large. En effet, l'article 9 évoquait des exemptions pour les seuls traitements effectués à des fins de journalisme. Celles-ci sont reprises au paragraphe 2 de l'article 85 et énoncent la même condition de conciliation avec la liberté d'expression. Là où nous voyons un élargissement potentiel de la portée de ce régime dérogatoire, c'est, dans le paragraphe 1^{er} de l'article 85, une disposition qui n'était pas en tant que telle présente dans la directive 95/46/CE. Affirmer que « [l]es États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information », c'est *in fine* permettre des dérogations potentielles pour protéger cette liberté, entendue plus largement que lors des seuls traitements à des fins journalistiques. L'article 85, § 1^{er}, précise d'ailleurs que cette conciliation se fait avec la liberté d'expression « y compris le traitement à des fins journalistiques ». Ainsi, un État pourrait parfaitement prévoir, si nous lisons correctement la disposition, des exemptions au règlement européen en vue de protéger la liberté d'expression et d'information, alors même que le traitement ne serait pas effectué aux fins de journalisme. Autrement dit, dans le cadre d'une action introduite à l'encontre d'un exploitant d'un moteur de recherche, le droit au déréférencement pourrait être tenu en échec en présence d'une exception nationale, validée grâce à l'article 85, § 1^{er}, en vue de protéger la liberté d'expression dans sa dimension d'accès du public à l'information.

C. Le déréférencement dans la pratique : l'analyse des critères

12. Des guidelines pour une mise en pratique. À la suite de l'arrêt *Google Spain*, le Groupe de travail « Article 29 » a développé des lignes directrices permettant une implémentation uniformisée de l'arrêt de la Cour de justice de l'Union européenne²⁹. Constatant, dans la première partie, les enseignements

²⁹ Art. 29 Data Protection Working Party, *Guidelines on the implementation of the Court of justice of the European Union judgement on « Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González »* C-131/12, document WP 225, 26 novembre 2014.

évoqués ci-avant, ces *guidelines* sont intéressantes dans leur seconde partie en ce qu'elles reprennent, sous forme d'un tableau, la liste de treize principaux critères – exposés sous forme de questions – à prendre en compte pour que la balance des intérêts évoqués dans l'arrêt soit correctement effectuée³⁰. Elles rappellent, en outre, que la demande de déréfèrement doit initialement être faite directement auprès du moteur de recherche. Ce n'est qu'en cas de refus de sa part que l'on peut se retourner vers les autorités nationales de contrôle des données ou les autorités judiciaires³¹. Certains d'ailleurs critiquent le fait que cette balance des intérêts soit effectuée, en première ligne, par le moteur de recherche lui-même, considérant que l'on fait peser là une responsabilité importante sur le responsable de traitement³². Certes, mais un parallèle pourrait être effectué avec un éditeur de presse qui, lui aussi, exécute une telle balance lorsqu'il prend la décision de publier des informations potentiellement attentatoires à la vie privée des individus. En outre, la décision éventuelle de refus de la part du moteur de recherche n'est pas irrévocable dès lors qu'un recours peut être introduit devant les autorités judiciaires ou de contrôle des données. Les lignes directrices soulignent ensuite que cette liste de critères constitue « *a flexible working tool* ». Sans que l'on puisse considérer qu'un élément est, en soi, déterminant, le texte soutient que chaque cas d'espèce implique l'application de plusieurs critères. Enfin, les *guidelines* mentionnent encore que « *each criterion has to be applied in the light of the principles established by the CJEU and in particular in the light of the "interest of the general public in having access to [the] information"* ». L'on s'interroge sur le sens à donner à cette mise en garde : faut-il y voir une tentative de relativisation de la hiérarchie mise en place par la Cour de justice des intérêts en présence (intérêts économiques, protection de la vie privée, intérêt du public à accéder à l'information) ?

Cela étant, malgré le développement de ces critères, la mise en pratique de ce droit reste complexe. Google³³ le reconnaît : dans son rapport relatif aux trois premières années d'application de ce que la société dénomme le *Right to be Forgotten*, Google souligne la complexité de mettre en œuvre cette balance des intérêts entre le droit à la vie privée, d'une part, et l'intérêt du public à pouvoir accéder à des informations, d'autre part³⁴. L'entreprise américaine avait d'ail-

³⁰ Voy. aussi CNIL, *Droit au déréfèrement. Les critères communs utilisés pour l'examen des plaintes*, www.cnil.fr. Il s'agit d'un bref commentaire des critères proposés par le Groupe de travail Article 29. L'analyse succincte des critères effectuée dans cette contribution s'inspire, pour partie, de ce document.

³¹ Voy. aussi The Advisory Council to Google on the Right to be Forgotten, 6 février 2015, p. 4.

³² A ce propos, voy. The Advisory Council to Google on the Right to be Forgotten, 6 février 2015, p. 18. Le rapport justifie ce rôle octroyé à Google de telle façon : « *[h]owever, assessing legal removal requests is already the norm for, and expected behavior of, search engines and other intermediaries in contexts outside data protection* ».

³³ Il y a lieu de préciser que l'entreprise Google n'est plus la société mère. En effet, depuis 2015, Google est devenue une filiale détenue à 100 % par Alphabet Inc. Dans un souci de clarification de nos propos et sans doute aussi par habitude, nous continuons cependant à nous référer dans ce texte à Google, conscients que cela n'est pas totalement correct sur le plan de l'arborescence des entreprises du groupe.

³⁴ T. BERTRAM *et al.*, *op. cit.*, p. 1.

leurs fait appel à un Comité consultatif composé d'experts afin de déterminer le cadre d'application du droit au déréfèrement. Un rapport est rendu public le 6 février 2015, celui-ci considérant que quatre critères doivent permettre à Google d'effectuer la balance des intérêts, sans que ces éléments soient hiérarchisés et sans qu'aucun de ces éléments ne soit déterminant.

Les lignes qui suivent ont vocation à présenter les critères des *guidelines*, ceux-ci recoupant les critères évoqués par le Comité consultatif mis en place par Google.

13. Critère 1 : les résultats de recherche sont-ils relatifs à une personne physique ? Le résultat apparaît-il à la suite d'une recherche effectuée à partir du nom de la personne concernée ? Cela appelle deux commentaires.

Premièrement, la question posée reflète, en réalité, une condition d'application de la réglementation relative aux données personnelles. En effet, le règlement européen ne s'applique qu'aux personnes physiques. L'article 1^{er}, alinéa 2, du règlement précise que « [l]e présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel ». Les personnes morales qui jouissent, elles aussi, d'un droit à la vie privée³⁵ sont exclues des garanties offertes par le règlement. Cette exclusion se distingue de ce que permettait la directive 95/46/CE. En effet, l'harmonisation constituant un *minimum*, certains États ont étendu l'application du champ d'application de la directive aux personnes morales, malgré le fait que ces dernières ne soient pas évoquées dans le texte³⁶.

Deuxièmement, le critère rappelle le cas d'espèce de l'affaire *Google Spain* : il s'agit d'un particulier effectuant une requête sur un moteur de recherche à

³⁵ Sur la protection de la vie privée des personnes morales, voy. la jurisprudence de la Cour européenne des droits de l'homme qui reconnaît l'application des droits fondamentaux à de telles personnes. En matière de vie privée, l'on évoque, notamment, *l'e-réputation des entreprises*. Pour des développements en la matière, voy. not. F. COLANTONIO, « Analyse de l'e-réputation », in *Les entreprises et l'e-Business*, Waterloo, Kluwer, 2015, pp. 89-128 ; J. VILAIN, « Le "droit à l'oubli" : d'une protection des particuliers vers une extension aux entreprises ? », in *Les entreprises et l'e-Business*, *op. cit.*, pp. 155-188 ; A. FAVREAU, « Le droit à l'oubli appliqué aux personnes morales », in D. DECHENAUD (dir.), *Le droit à l'oubli numérique. Données nominatives – Approche comparée*, coll. Création Information Communication, Bruxelles, Larcier, 2015, pp. 113-142.

³⁶ A ce propos, voy. la question écrite n° 5-2709 posée par Guido de Padt (Open VLD) au ministre de la Justice, *Doc. parl.*, Sénat, 2010-2011, 12 juillet 2011. La réponse est apportée le 1^{er} décembre 2011. L'auteur de la question écrit, à propos de la protection des personnes morales par la directive, ceci : « [s]ans se prononcer à ce sujet, la directive actuelle laisse toutefois aux États membres la possibilité d'intégrer ou non les personnes morales dans leur législation en matière de protection des données à caractère personnel. Cette base volontaire se retrouve également dans la Convention 108 du Conseil de l'Europe [...] ». La plupart des États membres du Conseil de l'Europe, dont la Belgique, n'ont pas fait usage de cette possibilité. En Norvège, en Autriche, en Italie et au Danemark (en partie seulement), les personnes morales ont bel et bien le droit à la protection des données à caractère personnel ».

partir des nom et prénom d'une personne physique. Pour le Groupe de travail «Article 29», les pseudonymes et surnoms doivent aussi être pris en considération lorsque la personne peut établir qu'ils sont liés à son identité réelle. On peut y voir ici une limitation du champ d'application. En effet, seules les recherches menées à partir d'une identité – qu'elle soit réelle ou par le biais d'un surnom – semblent permettre le droit au déréférencement tel que consacré par la jurisprudence européenne. Est-ce à dire qu'il faudrait exclure toute autre recherche effectuée à partir de données à caractère personnel, permettant *in fine* d'identifier une personne physique ? Nous ne le pensons pas, sous peine de limiter drastiquement la portée de ce droit.

14. Critère 2 : s'agit-il d'une personne publique ? Le plaignant joue-t-il un rôle dans la vie publique ? Pour la Cour de justice, le déréférencement peut être refusé si le plaignant a joué un rôle dans la vie publique. Les *guidelines* nous enseignent que le critère doit être entendu plus largement que celui des «personnages publics», élément que l'on retrouve notamment dans le cadre de la jurisprudence de la Cour européenne des droits de l'homme. Cette distinction faite indirectement entre le personnage public et la catégorie plus large des personnes jouant un rôle dans la vie publique est intéressante en ce qu'elle permet, par exemple, de considérer qu'une personne au centre d'un procès médiatique peut être considérée comme appartenant à la seconde catégorie, sans pour autant entrer dans la première.

La résolution 1165 de l'assemblée parlementaire du Conseil de l'Europe définit les personnages publics comme étant «ceux» qui exercent des fonctions publiques et/ou utilisent des ressources publiques et, d'une manière plus générale, [tous ceux] qui jouent un rôle dans la vie publique, qu'il soit politique, économique, artistique, social, sportif ou autre³⁷. Quant à la notion de «rôle dans la vie publique», il n'existe pas de définition claire. Les lignes directrices précisent, à titre d'exemple, que les hommes politiques, les représentants officiels d'institutions, les hommes d'affaires, les personnes membres de professions réglementées peuvent être considérés comme ayant ce rôle dans la vie publique. Elles estiment que «*if there is an argument in favour of the public being able to search for information relevant to their public roles and activities*». Les éléments proposés demeurent assez vagues et peu précis. En outre, les *guidelines* semblent, dans un premier temps, considérer maladroitement que certaines catégories de personnes jouent d'office un rôle dans la vie publique. Une personne qui joue un rôle dans la sphère publique ne perd pas toute protection de sa vie privée et de ses données à caractère personnel. Les *guidelines* confirment cela dans un deuxième temps, tout en soulignant que le déréférencement sera difficile à justifier lorsque les données porteront sur des personnages publics et que lesdites informations seront étrangères à des questions d'ordre privé. Pour la CNIL, «[une

³⁷ Résolution 1165 (1998) de l'Assemblée parlementaire du Conseil de l'Europe sur le droit à la vie privée, § 7.

distinction doit être faite entre la nature des informations traitées», elle souligne cependant que, «d'une manière générale, le fait qu'elles concernent une personnalité publique milite pour maintenir leur référencement»³⁸.

Un élément à prendre en compte est le fait de savoir si l'accès à une information particulière permet au public de se protéger contre des comportements publics ou professionnels contestables. En effet, la divulgation de tels agissements entre dans la notion de débat d'intérêt général. En réalité, la question qui se pose est bien celle de la participation d'informations à ce débat d'intérêt public, compte tenu du fait que les données visées concernent une personne privée ou un personnage public. En l'absence d'un tel débat, le déréférencement devrait avoir lieu d'office pour la personne privée. En ce qui concerne le personnage public, d'autres critères pourraient être pris en compte, tels que le comportement antérieur de la personne visée avec les médias³⁹.

Le Comité consultatif composé d'experts mandatés par Google souligne que le rôle joué par la personne concernée dans la vie publique constitue le premier élément (sur les quatre qu'il propose) à prendre en compte dans la balance des intérêts, s'appuyant directement sur les enseignements de l'arrêt *Google Spain*. Trois sous-catégories sont ainsi proposées : les individus ayant un rôle clair dans la vie publique, les individus n'ayant pas de rôle apparent dans la vie publique, et, enfin, les individus ayant un rôle limité – ou dans un contexte particulier – dans la vie publique. Pour les premiers, une demande de déréférencement a peu de chance d'être justifiée. Pour les deuxièmes, en revanche, le déréférencement est plus facilement envisageable. En ce qui concerne la troisième catégorie, le Comité indique ceci : «*deleting requests from such individuals are neither less nor more likely to justify deleting, as the specific content of the information being listed is probably going to weigh more heavily on the deleting decision*»⁴⁰.

15. Critère 3 : le plaignant est-il mineur ? L'objectif est, semble-t-il, de protéger davantage les mineurs. Bien que cet élément ne soit pas tiré directement de l'arrêt *Google Spain*, le Groupe de travail «Article 29» précise que, lorsque la demande de déréférencement émane d'un mineur, le moteur de recherche doit, d'une manière générale, lui donner satisfaction. Autrement dit, il y a lieu de prendre en compte «l'intérêt supérieur de l'enfant», lequel figure notamment à l'article 24 de la Charte des droits fondamentaux de l'Union européenne. Celui-ci dispose que, «dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale».

³⁸ CNIL, *Droit au déréférencement. Les critères communs utilisés pour l'examen des plaintes*, op. cit., p. 4.

³⁹ Cet élément est traduit notamment dans certaines dispositions du nouveau règlement. Voy. l'article 9, § 2, e), qui précise que l'interdiction de traiter des données sensibles n'est plus d'application dès lors que «le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée».

⁴⁰ The Advisory Council to Google on the Right to be Forgotten, 6 février 2015, p. 8.

Cette volonté de protéger les enfants mineurs, c'est-à-dire âgés de moins de 18 ans, ne figure pas dans le texte de la directive 95/46/CE. En revanche, le Règlement général sur la protection des données adapte plusieurs dispositions tenant compte de la minorité de la personne concernée⁴¹. Il estime d'ailleurs, en son considérant 38, que « [l]es enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel ». Dans le considérant 58 relatif au principe de transparence, il est écrit que « [l]es enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre »⁴². L'article 6, dont il a été question ci-avant et qui concerne la licéité du traitement, précise que la balance des intérêts devant être réalisée est à faire « notamment lorsque la personne concernée est un enfant ». Sans être précise, l'expression a au moins l'intérêt de rappeler le statut particulier des enfants dans la protection accordée. L'article 8 est entièrement dévolu aux enfants, puisqu'il porte sur les « [c]onditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information ». Il précise notamment que le consentement donné par un mineur pour un traitement de données doit être, lorsque l'enfant est âgé de moins de 16 ans, « donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant » (art. 8, al. 1^{er}).

16. Critère 4 : les données sont-elles exactes ? Lorsque des données en ligne sont inexactes, le déréférencement doit pouvoir être appliqué dès lors que la personne concernée fournit les informations utiles et nécessaires pour confirmer leur inexactitude. N'entrent pas dans cette catégorie des éventuelles opinions qu'une personne relaterait sur un autre individu. L'inexactitude porte ici sur des éléments factuels⁴³. Selon les lignes directrices, le déréférencement peut être plus facilement octroyé en cas de données inexactes, inadéquates ou trompeuses à l'égard d'une personne physique.

17. Critère 5 : les données sont-elles pertinentes et/ou excessives ?

Cette question extrêmement large s'inscrit, à nouveau, dans le fait que l'information participe au débat d'intérêt général. En outre, les *guidelines* s'intéressent à l'âge des données. Ainsi, elles admettent que l'écoulement du temps peut influencer sur la pertinence des informations diffusées. Nous le verrons par la suite, le critère de l'écoulement du temps est pris en compte par la jurisprudence

⁴¹ Outre les articles cités ci-après, voy. aussi l'article 40, § 2, g), et l'article 57, § 1^{er} b), du règlement. Sur ce sujet, voy. aussi l'article 12, alinéa 1^{er}, du règlement.

⁴² Voy. à ce propos, la traditionnelle distinction faite par la Cour européenne des droits de l'homme entre les constatations de fait et les jugements de valeur. Sur ce sujet, voy. not. F. JONGEN et A. STROWEL, avec la collaboration d'E. CRUYSMANS, *Droit des médias et de la communication. Presse, audiovisuel et Internet. Droit européen et belge*, coll. Création Information Communication, Bruxelles, Larcier, 2017, pp. 346-349, n° 511-515.

dans le traitement des requêtes d'anonymisation d'informations (voy. *infra*, n° 36).

La pertinence ou l'excessivité des données repose elle-même sur trois sous-critères :

- le premier implique de distinguer les informations relatives à la vie privée et les informations relatives à la vie professionnelle. Certaines données sont, en effet, d'ordre personnel, mais sans être d'ordre privé. À ce propos, les lignes directrices reviennent, de manière étonnante, sur le débat relatif aux personnalités publiques, question liée à un critère précédemment examiné. Elles soutiennent qu'une information d'ordre professionnel peut plus facilement être légitimement référencée, et le demeurer. Cela étant, il faut encore vérifier si les données ne sont pas excessives et si la personne concernée travaille toujours au même endroit, ceci revenant concrètement à poser la question de l'exactitude de l'information ;
- le deuxième sous-critère porte sur l'éventuelle atteinte à l'honneur, dans son sens pénal, que peut contenir l'information. Autrement dit, dès lors qu'une décision de justice confirme le caractère injurieux, diffamatoire, calomnieux, discriminatoire, etc., le déréférencement doit pouvoir être imposé. Sans une décision judiciaire, les autorités de contrôle en matière de données personnelles sont seules habilitées à vérifier l'excessivité des données ;
- enfin, le troisième sous-critère revient sur la distinction à faire entre les jugements de valeur et les constatations factuelles. Face à des opinions, voire même à des campagnes de dénigrement, les autorités de contrôle ne doivent pas systématiquement aboutir à prononcer le déréférencement des informations⁴⁴.

Le temps est un élément avancé par le Comité consultatif de Google pour évaluer une requête en déréférencement, reprenant le raisonnement tenu par la Cour de justice⁴⁵. Cet élément n'est cependant pas pertinent lorsque la demande de déréférencement porte sur des informations d'importance publique, tels des crimes contre l'humanité⁴⁶. L'on voit poindre ici le débat relatif au devoir de mémoire, ce dernier permettant de s'opposer à toute mise en œuvre d'un oubli, que cela soit sous la forme du déréférencement, de l'effacement ou de l'anonymisation. Le rapport du Comité consultatif souligne que ce facteur temporel est important notamment dans le cadre d'affaires pénales. En cela, il

⁴⁴ Il est intéressant de noter que les *guidelines* du Groupe de travail « Article 29 » écrivent que « [a]lthough the availability of such information may be hurtful and unpleasant, this does not necessarily mean that DPAs will consider it necessary to have the relevant search result de-listed » ; alors que l'analyse des critères faite par la CNIL souligne, en parlant de ces campagnes, qu'« après analyse des éléments de contexte, le déréférencement peut apparaître justifié, sans caractère systématique » (CNIL, *Droit au déréférencement. Les critères communs utilisés pour l'examen des plaintes*, op. cit., p. 6).

⁴⁵ Voy. le paragraphe 94.

⁴⁶ The Advisory Council to Google on the Right to be Forgotten, 6 février 2015, p. 14.

rejoint ce qui est évoqué ci-avant, ainsi que le critère 13 abordé ci-après relatif au caractère pénal de l'information litigieuse (voy. *infra*, n° 25). Le rapport indique que « [t]he severity of a crime and the time passed may together favour delisting, such as in the case of a minor crime committed many years in the past ». En revanche, dans d'autres situations, il pourrait y avoir un intérêt public permanent à accéder à l'information. Le rapport précise enfin que ce facteur temporel peut affecter le rôle public qu'une personne a eu à un moment donné avant de quitter cette vie publique.

18. Critère 6 : l'information est-elle sensible au sens de l'article 8 de la directive 95/46/CE ? L'article 8 de la directive considère comme sensibles les données « qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle ». La disposition interdit le traitement de ces données, cette interdiction étant cependant assortie d'un nombre important d'exception. Le même prescrit est repris à l'article 9, § 1^{er}, du règlement, celui-ci ajoutant à la liste des données dites sensibles les informations génétiques et biométriques, ainsi que les données relatives à l'orientation sexuelle d'une personne.

Compte tenu de leur impact important sur la vie privée ainsi que de l'interdiction de principe d'effectuer des traitements sur ces données dites sensibles, les autorités de contrôle ou judiciaires doivent être plus enclines à admettre leur déréférencement.

Le Comité consultatif de Google considère que la nature de l'information constitue un autre élément devant être pris en compte. Deux catégories d'informations sont distinguées. La première concerne des informations présentant un fort caractère privé. Il s'agit des informations relatives à la vie sexuelle, à la situation financière, à l'identification (par exemple, numéros de téléphone ou de carte d'identité), des informations considérées comme sensibles par la réglementation européenne en matière de protection des données, des informations privées sur des mineurs, des données fausses, inexactes ou présentant un risque, ainsi que de celles qui augmentent les intérêts privés d'une personne parce que cette dernière apparaît dans une image ou une vidéo. La deuxième catégorie regroupe les informations considérées comme étant d'intérêt public. Il s'agit de données politiques, de gouvernance ou relatives à un engagement citoyen, des débats religieux ou philosophiques, des informations relatives à la protection des consommateurs et à la santé publique, des informations relatives à l'activité criminelle, de celles qui contribuent au débat d'intérêt général, des données factuelles et exactes, des informations historiques, ainsi que des informations ayant trait à la recherche scientifique ou à l'expression artistique. Cette catégorisation faite par le Comité consultatif correspond *grosso modo* aux critères proposés par les *guidelines* du Groupe de travail « Article 29 ». En outre, les types d'informations énumérés semblent, en partie, s'appuyer sur les catégories tradi-

tionnelles de discours que l'on retrouve dans la jurisprudence de la Cour européenne des droits de l'homme⁴⁷.

19. Critère 7 : l'information est-elle à jour ? L'information a-t-elle été rendue disponible plus longtemps que nécessaire pour le traitement ? La question posée ici est celle de l'actualité de l'information. Peut-on, en d'autres termes, justifier le maintien de données en ligne dès lors que cette information participe encore et toujours à l'actualité ? Si tel est le cas, le déréférencement se justifie moins. En revanche, une information qui serait prémée au regard de son actualité a des chances plus importantes d'être déréférencée. La CNIL précise que « [c]ette analyse s'effectue en prenant en compte le contexte initial de mise en ligne et l'objectif poursuivi par la diffusion du contenu concerné »⁴⁸. Elle poursuit en proposant l'exemple d'« [u]n plaignant [qui] demande le déréférencement d'une information en ligne relative à une condamnation pénale, alors qu'il a depuis fait l'objet d'une relaxe en appel ».

20. Critère 8 : le traitement de l'information cause-t-il un préjudice au plaignant ? Les données ont-elles un impact négatif disproportionné sur la vie privée du plaignant ? L'arrêt de la Cour de justice a clairement établi qu'il n'était pas nécessaire de démontrer l'existence d'un préjudice pour pouvoir bénéficier du droit au déréférencement. Le paragraphe 96 de la décision mentionne que « la constatation d'un tel droit ne présuppose pas que l'inclusion de l'information en question dans la liste de résultats cause un préjudice à la personne concernée ». Cela étant, en cas de dommage subi par la personne concernée, dommage qui sera la plupart du temps d'ordre moral, le déréférencement semble pouvoir plus aisément se justifier. En outre, les *guidelines* mettent en garde contre l'impact néfaste que des informations, parfois mineures, peuvent avoir sur la vie privée d'un individu. Ainsi, « [t]he data might have a disproportionately negative impact on the data subject where a search result relates to a trivial or foolish misdemeanour which is no longer – or may never have been – the subject of public debate and where there is no wider public interest in the availability of the information ».

21. Critère 9 : les informations issues du moteur de recherche créent-elles un risque pour le plaignant ? La présence d'informations en ligne peut être la source d'un risque pour la personne visée. Ainsi, des données peuvent amener des personnes à harceler ou à voler l'identité d'un autre internaute. Lorsque le risque est substantiel – toute la difficulté résidant dans la détermination de ce caractère substantiel –, les autorités de contrôle doivent admettre que le déréférencement constitue une solution pour le limiter, voire le supprimer.

⁴⁷ À ce sujet, voy. F. JONGEN et A. STROWEL, avec la collaboration d'E. CRUYSMANS, *Droit des médias et de la communication. Presse, audiovisuel et internet. Droit européen et belge*, op. cit., pp. 70-81, n° 91-116, et pp. 325-365, n° 482-544.

⁴⁸ CNIL, *Droit au déréférencement. Les critères continus utilisés pour l'examen des plaintes*, op. cit., p. 7.

22. Critère 10 : dans quel contexte l'information a-t-elle été publiée?

Le contexte de la diffusion des informations est essentiel. Ainsi, il est nécessaire de s'interroger sur le caractère volontaire ou non de la divulgation. En effet, lorsque la personne concernée a volontairement diffusé des données qu'elle souhaite *in fine* être déréférencées, il y a lieu de partir du postulat qu'elle y a, dans un premier temps, consenti. Le consentement est défini comme étant « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement » (art. 4, 11), du règlement). Le consentement rend licite le traitement de données, comme le souligne l'article 6, § 1^{er}, a), du règlement. Cela étant, le règlement prévoit qu'un consentement valablement donné puisse être, dans un second temps, retiré. Tel est notamment le cas de l'article 17, § 1^{er}, b), du règlement qui prévoit que le droit à l'effacement est possible lorsque la personne concernée retire son consentement. Un tel retrait implique que le traitement n'est plus justifié sur un fondement licite, sauf à s'appuyer sur l'un des autres motifs de validité repris dans le règlement. Cela étant, l'article 17, § 1^{er}, b), permet d'obtenir l'effacement des données litigieuses auprès de l'éditeur de la page Web sur laquelle sont reprises ces informations. En l'espèce, les *guidelines* rappellent que le déréférencement des informations est indépendant d'une telle demande d'effacement. Pour le Comité consultatif Google, « [i]nformation that is published by or with the consent of the data subject himself or herself will weigh against delisting. This is especially true in cases where the data subject can remove the information with relative ease directly from the original source webpage ».⁴⁹ Nous estimons que cette dernière conclusion fait l'impasse sur la distinction claire faite dans l'arrêt *Google Spain* entre la responsabilité du moteur de recherche et celle de l'éditeur d'une page Web. Cette distinction ne doit pas être interprétée comme permettant d'agir contre l'un ou l'autre. Les traitements de données sont différents et se fondent sur des motifs distincts. Dès lors, des requêtes peuvent être adressées indépendamment ou simultanément à l'un ou l'autre.

Outre le caractère volontaire de la publication, il faut s'interroger sur son caractère initialement public : la personne concernée pouvait-elle s'attendre à ce que des données soient rendues publiques sur Internet ? Une divulgation à son insu pourrait justifier plus facilement le déréférencement des informations litigieuses. La CNIL propose un contre-exemple ne justifiant pas le déréférencement : il s'agit d'« [u]n plaignant [qui] demande le déréférencement d'un article concernant les résultats des élections municipales alors qu'il figure sur une des listes d'un parti politique et devait s'attendre à une diffusion de l'information ».⁵⁰

⁴⁹ The Advisory Council to Google on the Right to be Forgotten, 6 février 2015, p. 13.

⁵⁰ CNIL, Droit au déréférencement. Les critères communs utilisés pour l'examen des plaintes, op. cit., p. 8.

23. Critère 11 : le contenu a-t-il été rendu public à des fins journalistiques?

La finalité journalistique de la diffusion de données est importante dès lors qu'il existe un régime dérogatoire à des dispositions du règlement lorsque le traitement est effectué à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire (art. 85 du règlement [voy. *supra*, n^{os} 7 et 11]). L'objectif est louable : protéger la liberté d'expression et la liberté de la presse et, *in fine*, éviter que l'on puisse trop facilement restreindre le rôle de la presse en s'opposant aux traitements de certaines informations.

Les *guidelines* considèrent que cette finalité doit être prise en compte dans l'analyse d'une requête en déréférencement. Cela étant, « *this criterion alone does not provide a sufficient basis for refusing a request, since the ruling clearly distinguishes between legal basis for publication by the media, and the legal basis for search engines to organise search results based on a person's name* ». La CNIL nous paraît moins claire à ce sujet : elle précise que la présence d'une finalité journalistique « ne saurait conduire d'une manière systématique à refuser un déréférencement. Ce critère doit être combiné avec d'autres, par exemple, celui de la durée de la diffusion ou du préjudice pour la personne concernée ».⁵¹

Si l'on se réfère à l'arrêt *Google Spain*, et si l'on prend en compte ce qui transparaît dans l'extrait cité des lignes directrices, il nous semble qu'il faut considérer que les moteurs de recherche, lorsqu'ils effectuent un traitement de données à caractère personnel, ne sont pas mus par une finalité journalistique, mais davantage par une finalité économique. Dans son paragraphe 85, la Cour qui distingue clairement les traitements effectués par les moteurs de recherche des traitements effectués par les éditeurs de site Web souligne que ces derniers, « consistant dans la publication d'informations relatives à une personne physique », peuvent être, « le cas échéant », effectués « aux seules fins de journalisme ». Dès lors, le critère ne nous semble pas devoir être pris en compte dans l'analyse d'une demande d'application du droit au déréférencement, sauf à confondre les rôles respectifs des acteurs et intermédiaires présents sur Internet. En revanche, ce critère est fondamental lorsque la demande est adressée directement à l'éditeur d'un site Web afin de requérir, par exemple, une anonymisation des informations. Cela étant, l'article 85 nous paraissant élargir le champ des dérogations, comme nous l'avons explicité ci-avant (voy. *supra*, n^o 11), l'inscription par des États membres d'exemptions en faveur de la liberté d'expression pourrait faire obstacle à des demandes en déréférencement.

Le Comité consultatif Google estime qu'il y a lieu de prendre en compte la source de l'information ainsi que l'élément qui a motivé sa diffusion. L'exemple pris est celui d'une entité journalistique divulguant une information en respectant la déontologie journalistique. Compte tenu de cette finalité, les individus ont un intérêt à pouvoir accéder à cette information.

⁵¹ *Ibid.*

24. Critère 12 : la publication de l'information répond-elle à une obligation légale ? L'auteur de la publication avait-il l'obligation de rendre cette donnée personnelle publique ? Le traitement peut être justifié sur une base légale : dans certains cas, des textes normatifs nationaux imposent certaines publications. Une telle obligation légale met-elle en échec toute demande de déréfèrement ? Les lignes directrices semblent le concevoir, du moins, dans un premier temps. En effet, elles évoquent le fait que les autorités de contrôle peuvent concevoir que le déréfèrement soit approprié alors même que le traitement est justifié – et toujours justifié – sur un fondement légal. La CNIL émet une réserve similaire : « la combinaison avec d'autres critères (durée, préjudice...) et le fait qu'il convient de distinguer le réféfèrement d'une information par un moteur de recherche de sa diffusion publique pourrai[n]t, dans certains cas, jouer en faveur d'un déréfèrement »⁵². La distinction rappelée par la CNIL est essentielle et renvoie au raisonnement tenu pour le critère précédent. À nouveau, il n'y a pas lieu de confondre le traitement du moteur de recherche et le traitement de l'éditeur du site Web. Il nous semble que l'obligation légale justifie ce dernier traitement, mais qu'elle ne peut d'office constituer la justification du traitement effectué par le moteur de recherche. Dès lors, la prise en compte de cette obligation légale ne peut constituer un critère décisif : il nous semble, s'il doit être pris en compte, constituer un élément secondaire.

Dans l'affaire *Google Spain*, la publication des informations dans le quotidien *La Vanguardia* était légalement justifiée (§ 16) dès lors qu'elle avait été faite sur ordre du ministère du Travail et des Affaires sociales dans le cadre d'une procédure en recouvrement de dettes de sécurité sociale. Et, pourtant, les juges européens n'ont, dans leur raisonnement, pas pris en compte cette justification légale, sauf à considérer que les informations n'étaient pas inexacts et n'avaient pas été diffusées illicitement. Seul le fait que le traitement fût nécessaire à la réalisation de l'intérêt légitime de Google est pris en compte dans le raisonnement proposé par les juges, les obligeant à mettre en balance les intérêts de chaque partie, comme l'impose l'article 7, f), de la directive.

25. Critère 13 : l'information est-elle relative à une infraction pénale ? Les règles relatives à la diffusion d'informations relatives à des infractions pénales sont propres à chaque État membre. Le Groupe de travail « Article 29 » considère que les autorités de contrôle doivent pouvoir admettre plus facilement le déréfèrement lorsque les informations portent sur des délits mineurs et que ceux-ci se sont passés il y a un certain temps. Le facteur temporel joue un rôle important, ainsi que la gravité de l'infraction. Les *guidelines* sont cependant prudentes puisqu'elles rappellent qu'il y a lieu de traiter ces demandes de déréfèrement avec prudence et au cas par cas.

⁵² Ibid., p. 9.

À cet égard, l'article 10 du règlement indique que « [l]e traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique ». La prudence des lignes directrices s'explique sans doute par les restrictions apportées par l'article 10 du règlement (et, précédemment, l'article 8, § 5, de la directive) au traitement de ces données.

26. La balance des intérêts en pratique : l'expérience de Google à travers quelques chiffres. Le Comité consultatif Google a donné plusieurs indications sur la procédure à mettre en place par Google pour que les requêtes en déréfèrement puissent être traitées efficacement par le géant américain. Il faut, en effet, que les personnes concernées donnent suffisamment d'informations pour faciliter l'exécution de cette balance des intérêts.

L'entreprise Google a diffusé, début 2018, un rapport faisant état de l'application du droit au déréfèrement depuis le prononcé de l'arrêt *Google Spain*. Elle y dresse un premier bilan se fondant sur les 2,4 millions de demandes de déréfèrement qui lui sont parvenues durant ces trois premières années et demie d'application de ce droit⁵³. Le tiers (33 %) des demandes porte sur du contenu publié sur les réseaux sociaux. Sur l'ensemble des demandes de déréfèrement, plus de 77 % portent sur des URL dont l'extension (.be, .fr, .it...) est la même que le pays duquel provient le demandeur. Plus de la moitié des demandes (51 %) provient de France, du Royaume-Uni et d'Allemagne. Les demandes introduites en Belgique concernent 2,8 % de l'ensemble des requêtes reçues par Google. Quant à la validation par le moteur de recherche de ces requêtes, seuls 43 % des URL rencontrent les différents critères proposés et sont, en définitive, déréférés. Quatre-vingt-cinq pour cent des demandes proviennent de personnes privées n'étant pas des figures publiques. La proportion de requêtes introduites par des mineurs ne s'élève, elle, qu'à 5,4 %.

Le délai de traitement d'une demande par Google est, depuis le 1^{er} janvier 2017, de quatre jours. Il était de quatre-vingt-cinq jours pendant les premiers mois d'application du droit au déréfèrement, ce délai s'expliquant par la nécessité d'intégrer la procédure, les critères, ainsi que de déterminer ce qu'il faut entendre par « informations inexacts, inadéquates, non pertinentes ou excessives ».

⁵³ Le rapport se base sur les demandes introduites entre le 30 mai 2014 et le 31 décembre 2017.

D. Le déréférencement, un droit encore en devenir

27. Un droit en chantier. Beaucoup de points d'ombre subsistent et la délimitation précise des contours du droit au déréférencement exigera encore des précisions, notamment de la jurisprudence. Signalons que la Cour de justice de l'Union européenne a été saisie de questions préjudicielles posées par le Conseil d'État français en vue de clarifier ce droit au déréférencement.

Dans une première affaire⁵⁴, la première question porte sur le fait de savoir « dans quelle mesure l'interdiction de traitement de données sensibles et de données relatives aux infractions, condamnations pénales ou aux mesures de sûreté[s] s'applique aux moteurs de recherche en tant que responsable[s] du traitement »⁵⁵. Dans l'hypothèse où la Cour serait amenée à reconnaître que cette interdiction s'applique aux moteurs de recherche, le Conseil d'État français pose alors plusieurs questions complémentaires. En bref, il s'interroge sur la possibilité de refuser une demande de déréférencement en se fondant sur les exceptions rendant envisageable le traitement de données sensibles ou sur la dérogation prévue pour les traitements à des fins de journalisme. Si ce droit au déréférencement ne peut être refusé sur la base de ces motifs, la juridiction administrative française s'interroge alors sur les obligations devant être remplies par les moteurs de recherche pour mettre en œuvre cette désindexation.

Dans une seconde affaire⁵⁶, la problématique touche le champ d'application territorial du droit au déréférencement. La première question est formulée comme suit : faut-il interpréter ce droit comme impliquant le déréférencement « sur l'ensemble des noms de domaine [...] de telle sorte que les liens litigieux n'apparaissent plus quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée, y compris hors du champ d'application territorial de la directive du 24 octobre 1995 » ? La question est évidemment fondamentale en ce qu'elle conditionne l'efficacité même du droit au déréférencement. La deuxième question se pose en cas de réponse négative de la part de la Cour de justice à la première interrogation. Elle demande si le déréférencement peut alors s'appliquer à l'ensemble des extensions nationales correspondant aux États membres de l'Union européenne ou s'il doit seulement être appliqué sur les résultats d'une recherche réalisée sur la version du site correspondant à l'État où la demande a été effectuée. La troisième et dernière ques-

⁵⁴ Demande de question préjudicielle présentée par le Conseil d'État (France) le 15 mars 2017, G. C. A. F. B. H., E. D. c. *Commission nationale de l'informatique et des libertés* (CNIL), C-136/17. La décision du Conseil d'État date du 24 février 2017 (C.E. fr. 24 février 2017, Mme C., M.F. M.H., M.D., n° 391000, 393769, 399999 et 401258, www.legifrance.gouv.fr).

⁵⁵ O. TAMBOU, « Trois enseignements à tirer de la mise en œuvre juridictionnelle de l'arrêt *Google en France* », *E-Conferrence, droit à l'oubli en Europe et au-delà*, [www.blogdroiteuropeen.com](http://blogdroiteuropeen.com), mis en ligne en mai 2017, p. 5.

⁵⁶ Demande de décision préjudicielle présentée par le Conseil d'État (France) le 21 août 2017, *Google Inc. c. Commission nationale de l'informatique et des libertés* (CNIL), C-507/17.

tion s'interroge sur l'application des techniques de « géo-blocage » dans la suppression des résultats litigieux.

Section 2

Le droit à l'anonymisation ou à la pseudonymisation

28. Introduction. Les requêtes visant à anonymiser ou pseudonymiser des informations personnelles relèvent également du « droit à l'oubli ». Les actions introduites devant les juridictions belges le sont généralement à partir d'une action en responsabilité civile extracontractuelle. À la différence du droit au déréférencement, les actions ne sont plus introduites à l'égard du responsable du moteur de recherche, mais à l'encontre d'un éditeur de site Web. À nouveau, comme pour ce qui concerne le droit au déréférencement, la jurisprudence a joué un rôle fondamental dans l'implémentation d'un droit à l'anonymisation comme moyen de réparation d'un préjudice subi à la suite d'une atteinte au droit à la vie privée (sous-section 3). En outre, il importe d'indiquer préalablement les raisons qui expliquent le passage par l'action en responsabilité civile extracontractuelle, et non la possibilité de prendre appui sur les dispositions en matière de protection des données à caractère personnel. En effet, l'existence, dans ces textes, d'une dérogation en faveur des traitements exécutés à des fins de journalisme rend difficile et incertaine l'application de ces dispositions (sous-section 2).

Sous-section 1

Définir l'anonymisation et la pseudonymisation

29. Qu'est-ce que la pseudonymisation ? Outre le droit au déréférencement, les actions introduites pour des atteintes au droit à la vie privée et au droit à la protection des données personnelles peuvent aboutir à l'invocation d'un droit à l'anonymisation, voire à la pseudonymisation. Cette dernière notion fait l'objet d'une définition dans le règlement : il s'agit de traiter les « données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » (art. 4, 5), du règlement).

L'exception de journalisme : le motif d'exclusion de la réglementation relative aux données à caractère personnel

30. L'ordonnance du 9 octobre 2012 : comment comprendre l'exception de journalisme ? Le 9 octobre 2012⁵⁷, le président du Tribunal de première instance de Bruxelles a rendu une ordonnance relative à une demande de retrait de l'identité d'une personne dont les nom et prénoms apparaissent dans un article relatant des condamnations judiciaires antérieures à 2004, pour des faits datant des années 1990, voire avant. Le demandeur invoque son « droit à l'oubli », celui-ci ne faisant toutefois l'objet d'aucun développement dans l'ordonnance. En effet, la demande de retrait prend pour fondement législatif la réglementation belge relative à la protection des données à caractère personnel, soit la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel⁵⁸. L'application de ce texte est rapidement confirmée par l'ordonnance, le président du tribunal estimant qu'il y a bien un traitement de données : des archives en ligne comprenant des noms et prénoms de personnes, rendues disponibles grâce aux moteurs de recherche, constituent un traitement, en l'espèce automatisé. Le fait que les données aient déjà fait l'objet d'une publication préalable par d'autres médias n'a aucune incidence sur l'application de la loi. L'ordonnance confirme ainsi le raisonnement tenu par la Cour de justice de l'Union européenne, dans un arrêt du 16 décembre 2008, dans lequel la juridiction européenne énonce que des « activités de traitement de données à caractère personnel [...] qui ne comprennent que des informations déjà publiées telles quelles dans les médias relèvent du champ d'application de la directive 95/46/CE »⁵⁹.

Pour le demandeur, le traitement de données personnelles le concernant est interdit dès lors qu'il s'agit d'informations relatives à des procédures et condamnations judiciaires. L'article 8 de la loi du 8 décembre 1992 reprend, en effet, l'exception de l'article 8, § 5, de la directive (elle-même reprise à l'article 10 du règlement ; voy. *supra*, n° 25). Cela étant, cette interdiction de principe est assortie, comme il a été souligné ci-avant, d'un certain nombre d'exceptions, parmi

⁵⁷ Civ. Bruxelles (réf.), 9 octobre 2012, A.M., 2013/3-4, p. 267, note E. CRUYSMANS, « Le traitement de données à caractère personnel effectué à des fins de journalisme : la consécration de la liberté d'expression ».

⁵⁸ Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B., 18 mars 1993. La loi a ensuite été modifiée par une loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, M.B., 3 février 1999.

Voy. l'article 14 de la loi qui organise cette procédure particulière. Voy. aussi l'article 587, 4°, du Code judiciaire.

⁵⁹ CJUE (gde ch.), 16 décembre 2008, *Tietosuoja- ja valtuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*, C-73/07, R.D.T.I., 2010/38, p. 127, § 49, obs. C. DE TERWANGNE, « Les dérogations à la protection des données en faveur des activités de journalisme enfin élucidées » (R.D.T.I., 2010/38, pp. 121-144).

lesquelles le fait que le traitement soit effectué à des fins de journalisme⁶⁰. L'articulation de ces diverses dispositions amène le président du tribunal de première instance à se poser la question du champ d'application de cette exception, celle-ci mettant en péril l'interdiction de traitement d'informations judiciaires ainsi que d'autres prérogatives de la réglementation sur les données à caractère personnel. Établie dans le souci de concilier le droit à la vie privée et le droit à la liberté d'expression, l'exception est considérée par l'avocate générale Juliane Kokott comme permettant *in fine* de suspendre quasiment l'application de toute la directive européenne⁶¹. Cela étant, de la compréhension de la notion de « journalisme » dépend, pour partie, la portée de plusieurs dispositions figurant dans les normes sur la protection des données à caractère personnel. La loi belge du 8 décembre 1992 n'en dit mot. Sans doute le terme paraissait clair. Pourtant, le Conseil d'État avait suggéré de manière expresse, dans son avis préalable à la loi, que des précisions soient apportées à cette notion afin d'éviter tout problème ultérieur d'interprétation⁶².

Sans entrer largement dans le raisonnement mené par le président du tribunal de première instance de Bruxelles⁶³, ce dernier a considéré que la constitution d'archives en ligne participe à la finalité de journalisme, celle-ci ne se limitant « pas à rendre compte de l'actualité, mais contribue, par la diffusion d'informations, d'idées ou d'opinions et notamment celles contenues dans les archives des quotidiens, à alimenter le débat public ». Et de conclure que l'article 8 de la loi du 8 décembre 1992 ne peut, dès lors, trouver application en l'espèce. L'ordonnance poursuit cependant son raisonnement en s'interrogeant sur une éventuelle limite temporelle d'application de l'exception de journalisme. Dit autrement, le juge se demande si l'écoulement du temps a une influence sur le traitement des données conservées dans les archives. Dans une justification fort pragmatique, le président du Tribunal de première instance de Bruxelles conclut à une réponse négative. Rien n'oblige les personnes faisant œuvre de journalisme à procéder à l'anonymisation des données à caractère personnel après un certain laps de temps.

En conclusion, le constat est clair : requérir l'anonymisation d'archives en ligne en s'adressant à l'éditeur du site Web sur le fondement de la réglementation en matière de données personnelles risque de se voir opposer une fin de non-recevoir. Cet enseignement apparaît en filigrane dans l'arrêt *Google Spain* lorsque les juges européens distinguent la responsabilité de l'éditeur de celle du

⁶⁰ Art. 3, § 3, de la loi ; art. 9 de la directive 95/46/CE ; art. 85 du règlement n° 2016/679.

⁶¹ Concl. Av. gén. Juliane KOKOTT du 8 mai 2008, *Tietosuoja- ja valtuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*, C-73/07, §§ 57 et 60. Cécile de Terwangne souligne que les régimes dérogatoires transposés dans les pays de l'Union européenne diffèrent sensiblement (voy. C. de TERWANGNE, « Les dérogations à la protection des données en faveur des activités de journalisme élucidées », op. cit., pp. 135-137).

⁶² Avis du Conseil d'État, *Doc. parl.*, Chambre, 1997-1998, séance du 20 mai 1998, 1566/1, p. 188.

⁶³ Pour ce faire, nous renvoyons à E. CRUYSMANS, « Le traitement de données à caractère personnel effectué à des fins de journalisme : la consécration de la liberté d'expression », note sous Civ. Bruxelles (comme en réf.), 9 octobre 2012, A.M., 2013/3-4, pp. 270-273.

moteur de recherche, considérant notamment que le traitement effectué par le premier peut être justifié à des fins de journalisme⁶⁴.

31. La notion de journalisme dans le règlement. L'exception est principalement reprise à l'article 85 qui dispose en son paragraphe 1^{er} que son objectif est de concilier, « par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement 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 ». Outre cette disposition, l'article 17, § 3, a), relatif au droit à l'effacement précise que ce droit n'est pas d'application lorsque le traitement est effectué à des fins de « liberté d'expression et d'information ». Cette volonté de concilier une telle liberté et la protection des données est encore inscrite dans le considérant 153 du règlement⁶⁵. Dans cet équilibre à trouver, le considérant, outre l'audiovisuel, pointe, à titre d'exemple, le cas des « documents d'archives d'actualités et bibliothèques de presse »⁶⁶. La question est importante vu que la plupart des journaux traditionnels ont désormais un site Internet reprenant, souvent en libre accès, leurs archives. Quant à la notion même de journalisme, ce même considérant confirme sans nul doute son interprétation large, conclusion à laquelle était arrivé le président du Tribunal de première instance de Bruxelles dans l'ordonnance du 9 octobre 2012 évoquée ci-avant. En effet, le considérant souligne que, « [p]our tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique, il y a lieu de retenir une interprétation large des notions liées à cette liberté, telles que le journalisme ». À cet égard, il est intéressant de noter que le considérant 121 de la proposition de règlement, devenu le considérant 153 dans le règlement tel qu'adopté en 2016, ajoutait une définition qui a été supprimée. Selon cette définition, il fallait « qualifier de «journalistiques» les activités ayant pour objet de communiquer au public des informations, des opinions ou des idées, quel que soit le vecteur utilisé pour les transmettre. Il convient de ne pas limiter cette catégorie aux seules activités des entreprises de médias et d'y inclure tant celles qui poursuivent un but lucratif que celles qui n'en poursuivent pas ».

Tout ceci confirme l'étendue très – trop – large de l'exception en faveur du journalisme et de la liberté d'expression⁶⁷. Dès lors que l'interprétation de l'exception est large, le même constat que celui effectué en suivant le raisonnement tenu dans l'ordonnance du 9 octobre 2012 peut être fait : la réglementation relative à la protection des données à caractère personnel ne permet pas de pouvoir agir efficacement contre l'éditeur d'un site Web pour exiger qu'il anonymise des archives en ligne.

⁶⁴ Voy. le paragraphe 85 de l'arrêt *Google Spain*; voy. aussi *supra*, n° 4.

⁶⁵ Le considérant 153 semble faire clairement écho à l'article 85 du règlement.

⁶⁶ Cet élément était déjà inscrit dans le considérant 37 de la directive 95/46/CE.

⁶⁷ Voy. aussi *supra*, n° 7, 11 et 23.

A. La confirmation par la jurisprudence

32. Oubli, anonymisation et jurisprudence belge. À défaut de pouvoir s'appuyer sur le droit à la protection des données à caractère personnel, les demandeurs choisissent habituellement, comme pour d'autres atteintes au droit à la vie privée, une action civile en responsabilité extracontractuelle, considérant que la persistance d'informations personnelles sur le Web leur cause un préjudice nécessitant réparation. Plusieurs affaires peuvent être mentionnées, l'une d'entre elles ayant été portée devant la Cour de cassation. Certes, ces affaires sont moins retentissantes que l'arrêt *Google Spain*. Cela étant, elles sont précieuses dans la consécration de ce « droit à l'oubli » qui prend ici concrètement la forme d'une requête en anonymisation d'informations.

Ainsi, il y a lieu de citer une première décision rendue par le Tribunal de première instance de Neufchâteau datant du 25 janvier 2013⁶⁸, confirmée par la Cour d'appel de Liège le 25 septembre 2014⁶⁹, le raisonnement ayant ensuite été validé par la Cour de cassation en date du 29 avril 2016⁷⁰. Dans une seconde affaire, le Tribunal de première instance de Liège a rendu un jugement le 3 novembre 2014⁷¹, confirmé par un arrêt de la Cour d'appel de Liège du 4 février 2016⁷². Les faits de ces affaires sont assez simples et présentent des similitudes importantes. Les demandes portent sur l'anonymisation d'articles qui, publiés une première fois dans la presse écrite, sont nouvellement diffusés par le biais des archives numériques des éditeurs de presse. Alors que, dans les archives papier, ces articles avaient fort peu de chance d'être à nouveau consultés – ce qui *de facto* implique l'oubli –, le développement de l'accès gratuit des archives numériques permet à tout un chacun de retrouver facilement

⁶⁸ Civ. Neufchâteau (2^e ch.), 25 janvier 2013, J.L.M.B., 2013, p. 1182; A.M., 2013/6, p. 478, note. Le jugement accorde, en outre, un euro comme dédommagement du préjudice subi par le médecin.

⁶⁹ Liège (20^e ch.), 25 septembre 2014, A.M., 2015/3-4, p. 319, note; J.L.M.B., 2014, p. 1952, note E. CRUYSMANS, « Liberté d'expression, archives numériques et protection de la vie privée : la conciliation de trois réalités divergentes grâce au droit à l'oubli »; N.J.W., 2015/314, p. 26, note P. VAN ECKE et M. LE BOUDEEC, « Recht op vergetelheid ook van toepassing op krantenarchieven », R.G.D.C., 2016/5, p. 294, note E. MONTERO et Q. VAN ENIS, « Les métamorphoses du droit à l'oubli sur le net ».

⁷⁰ Cass. (1^{re} ch.), 29 avril 2016, A.M., 2016/5-6, p. 459, note M. CLÉMENT-FONTAINE, « Faut-il se réjouir de la percée du droit à l'oubli numérique ? », *Computer*, 2017/1, p. 31, note J. AUSLOOS, « Vergetelheidszaken voor de Hoven van Cassatie te België en Frankrijk – contradictio of complementair ? », J.T., 2016, p. 609, note E. CRUYSMANS, « Le droit à l'oubli devant la Cour de cassation », J.L.M.B., 2017/5, p. 208; N.J.W., 2016/350, p. 778, note E. BREWAEYS, « Identificatie van een moordenaar », R.D.C., 2017/2, p. 206, note J. CLINCK, « Het recht om (digitaal) vergeten te worden erkend door het Hof van Cassatie ».

⁷¹ Civ. Liège (4^e ch.), 3 novembre 2014, J.L.M.B., 2014/41, p. 1961, note E. CRUYSMANS, « Liberté d'expression, archives numériques et protection de la vie privée : la conciliation de trois réalités divergentes grâce au droit à l'oubli ».

⁷² Liège (20^e ch.), 4 février 2016, A.M., 2016/5-6, p. 462, note, J.L.M.B., 2017/5, p. 212; R.G.A.R., 2016/9, n° 15337, note.

ces écrits par le biais d'une requête à partir des seuls nom et prénom. Dans la première affaire, un médecin, ayant provoqué un accident mortel de la circulation alors qu'il conduit en état d'ébriété, est nommément cité dans un article du quotidien *Le Soir*. L'article, publié en 1994, relate plus globalement une série d'accidents mortels qui se sont déroulés en l'espace de quelques jours dans la région de Tournai, en nommant certaines personnes impliquées, notamment le médecin. Ce dernier, pénalement condamné tant en première instance qu'en degré d'appel, a fait l'objet d'une réhabilitation en 2006. Deux années plus tard, l'éditeur du quotidien décide de mettre en ligne la plupart de ses archives, offrant à tout internaute un accès gratuit à un nombre très important d'articles. Quant à la seconde affaire, ce sont, en réalité, deux procédures qui ont été jointes devant la juridiction de première instance en raison de leur connexité. La première concerne la diffusion d'un article dans le quotidien *La Libre Belgique* dont le contenu relate l'arrestation d'un membre de la « cellule Cools », du nom de l'ancien homme politique belge. L'article évoque une personne mêlée à une perquisition effectuée dans le cadre du dossier relatif à l'assassinat d'André Cools, perquisition durant laquelle plusieurs armes ont été découvertes. La suspicion est toutefois rapidement levée. L'autre cas concerne une tentative d'assassinat dans la région liégeoise. Le journaliste du quotidien *Le Soir*, évoquant une somme importante d'argent qui doit permettre de recruter le tueur, cite plusieurs noms et prénoms, dont ceux du demandeur, associé de près ou de loin dans le macabre projet.

Dans chacune de ces affaires, les demandeurs ne mettent pas en cause la licéité de la parution dans les versions papier des journaux. En revanche, ils considèrent que la permanence de la diffusion en ligne de ces articles non réactualisés constitue une atteinte à leur droit à l'oubli justifiant une première demande de suppression, ou, à tout le moins, d'anonymisation, adressée directement au quotidien⁷³. Se heurtant à un refus de faire droit à leur demande par les journaux respectifs, les demandeurs décident d'agir devant les juridictions belges en responsabilité civile extracontractuelle à l'encontre des éditeurs, l'objectif étant d'obtenir réparation d'un préjudice essentiellement moral.

33. L'arrêt de la Cour de cassation du 29 avril 2016. La Cour de cassation belge s'est prononcée le 29 avril 2016, validant le raisonnement tenu par les juridictions de fond. En réalité, la cour confirme que « [s]e droit au respect de la vie privée, garanti par les articles 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 17 du Pacte international relatif aux droits civils et politiques et 22 de la Constitution, qui [...] comporte le "droit à l'oubli" permettant à une personne reconnue coupable d'un crime ou d'un délit de s'opposer dans certaines circonstances à ce que son passé judiciaire soit rappelé au public à l'occasion d'une nouvelle divulgation des faits,

⁷³ Dans la première affaire évoquée, le médecin transmet, en outre, sa demande au Conseil de déontologie journalistique, celui-ci considérant cependant la plainte comme étant irrecevable.

peut justifier une ingérence dans le droit à la liberté d'expression ». Elle confirme le fondement de ce « droit à l'oubli » et estime, par conséquent, certes indirectement, que la combinaison de ces dispositions protectrices de ce droit fondamental et de l'article 1382 du Code civil permet d'agir devant les juridictions civiles pour obtenir réparation d'un préjudice subi à la suite d'une atteinte à ce droit fondamental.

Il est intéressant de mettre en perspective cet arrêt avec une décision rendue par la Cour de cassation française en date du 12 mai 2016⁷⁴. *A priori*, les affaires portent sur la même problématique, à savoir ce « droit à l'oubli »⁷⁵. Et, pourtant, à lire les deux décisions, l'impression première qui s'en dégage est une opposition totale : en Belgique, le droit à l'oubli serait valide, en France, il semblerait rejeté par la jurisprudence. En réalité, l'arrêt de la Cour de cassation belge se prononce sur l'existence d'un droit à l'oubli, entendu comme une composante du droit à la protection de la vie privée, tandis que la Cour de cassation française s'est prononcée sur ce « droit à l'oubli » en tant que partie intégrante de la réglementation en matière de protection des données personnelles. Cet angle différent justifie les résultats opposés.

B. Demander une anonymisation sur pied de l'article 1382 du Code civil

34. L'oubli comme fondement, l'anonymisation comme mode de réparation. Comme nous l'avons souligné ci-avant, les affaires évoquées *supra*, bien que se fondant sur le « droit à l'oubli », s'inscrivent sur le plan judiciaire dans une procédure en responsabilité extracontractuelle, impliquant l'existence des trois conditions traditionnelles, la faute, le dommage et le lien de causalité. L'analyse de la faute constitue sans nul doute la partie la plus intéressante du raisonnement effectué par la jurisprudence⁷⁶.

1. La faute

35. La persistance des informations. La faute constitue en réalité le fait, pour l'éditeur, d'avoir laissé subsister dans les archives numériques les noms de certaines parties alors même que des demandes d'anonymisation leur ont été transmises par les personnes visées. Autrement dit, la faute tient au refus d'accéder à la demande d'anonymisation. En cela, les demandeurs postulent que les éditeurs n'ont pas eu le comportement que tout autre éditeur suffisamment prudent et diligent, placé dans les mêmes circonstances, aurait adopté. C'est donc sous l'angle de l'éditeur en tant que « bon père de famille » que l'on se

⁷⁴ Cass. fr. (1^{re} ch. civ.), 12 mai 2016, n° 15.17729, disponible sur le site <https://www.legifrance.gouv.fr>.

⁷⁵ Pour un commentaire de ces deux affaires, voy. M. CLÉMENT-FONTAINE, « Faut-il se réjouir de la percée du droit à l'oubli numérique ? », *op. cit.*, pp. 453-459 ; T. LÉONARD, « Droit à l'oubli numérique : Belgique et France n'ont pas la même sensibilité », *L'Écho*, 6 juillet 2016, disponible sur le site www.lecho.be.

⁷⁶ Le raisonnement proposé ci-après est en partie inspiré des développements rédigés par Édouard Cruysmans (voy. « Liberté d'expression, archives numériques et protection de la vie privée : la conciliation de trois réalités divergentes grâce au droit à l'oubli », *op. cit.*, pp. 1972-1980).

place pour jauger de l'existence d'un comportement fautif. Dans les décisions citées précédemment, il est précisé en outre que la responsabilité des éditeurs doit s'apprécier au moment où les demandes d'anonymisation sont formulées, et non, comme on aurait pu le penser, au moment où ces demandes sont refusées.

Pratiquement, les juridictions ont en réalité intégré dans leur raisonnement relatif à cette première condition de la responsabilité civile extracontractuelle une balance des intérêts entre les droits fondamentaux en présence : d'une part, la liberté d'expression (consacrée par l'article 10 de la CEDH et par les articles 19 et 25 de la Constitution), de l'autre, le droit au respect de la vie privée (consacré par l'article 8 de la CEDH et par l'article 22 de la Constitution). Un tel *modus operandi* semble avoir été avalisé par la Cour de cassation. Elle souligne en effet que « la liberté d'expression et, partant, la liberté de la presse confèrent aux organes de la presse écrite le droit de mettre en ligne des archives numériques et au public celui d'accéder à ces archives ». Cela étant, cette liberté n'est point absolue : « [...] l'archivage numérique d'un article ancien de la presse écrite ayant à l'époque des faits, légalement relaté des événements du passé désormais couverts par le droit à l'oubli [...] n'est pas soustrait aux ingérences que ce droit peut justifier dans le droit à la liberté d'expression. Ces ingérences peuvent consister en une altération du texte archivé de nature à prévenir ou réparer une atteinte au droit à l'oubli⁷⁷. Ce conflit de droits fondamentaux se résout alors par l'exécution du test en trois étapes découlant de l'article 10, § 2, de la Convention. De cette analyse dépend l'existence ou non de la faute. Il y a, par conséquent, lieu de démontrer qu'il existe une ingérence prévue par la loi poursuivant un but légitime, et qu'elle est nécessaire dans une société démocratique. En l'espèce, l'ingérence (selon l'article 10 de la Convention, toutes « formalités, conditions, restrictions ou sanctions ») se matérialise dans la demande de suppression d'informations.

Sur la condition de légalité, la Cour de cassation, après avoir confirmé que le droit à l'oubli constitue une composante du droit à la vie privée, juge que la demande d'anonymisation, c'est-à-dire l'altération du texte initial, repose, en réalité, non pas sur un seul fondement légal, mais bien sur une combinaison de dispositions. Ainsi, la demande peut être fondée sur les articles 8 de la Convention, 22 de la Constitution et 1382 du Code civil : l'ensemble de ces dispositions permet d'obtenir une norme répondant aux critères à satisfaire selon la jurisprudence de la Cour de Strasbourg, à savoir une disposition de portée générale, claire, précise, prévisible et accessible⁷⁸. Autrement dit, les éditeurs sont à même de prévoir leur éventuelle condamnation par des juridictions

⁷⁷ La Cour de cassation semble considérer qu'une telle ingérence pourrait prévenir une atteinte au droit à l'oubli. Admettrait-elle que, sur ce fondement particulier, une ingérence de nature préventive puisse être prise ?

⁷⁸ À ce sujet, voy. F. JONGEN, A. STROWEL et E. CRUYSMANS (collab.), *Droit des médias et de la communication. Presse, audiovisuel et Internet. Droit européen et belge*, op. cit., pp. 316-320, n° 466-473.

civiles à anonymiser des articles en ligne sur la base de ces dispositions. La Cour européenne a d'ailleurs déjà validé ce type de fondement légal dans le cadre d'une mesure répressive⁷⁹. Soulignons que le demandeur en cassation soutenait que le droit à l'oubli ne bénéficiait d'aucune consécration légale, mais seulement de consécérations doctrinales et jurisprudentielles, visant plus particulièrement l'arrêt *Google Spain*⁸⁰. La Cour de cassation rejette ce raisonnement, affirmant que le droit à l'oubli constitue bien une composante particulière du droit à la vie privée.

Quant à la condition de légitimité, il ne fait aucun doute qu'une requête en anonymisation a vocation à protéger « les droits d'autrui » (art. 10, § 2, CEDH), en l'espèce le droit au respect de la vie privée, dans sa composante « droit à l'oubli ».

Enfin, la condition de proportionnalité : il y a lieu de vérifier si l'ingérence est « nécessaire dans une société démocratique », cette condition se décomposant en trois sous-étapes. *Primo*, l'adéquation de la mesure n'implique pas de longs développements dès lors que la mesure permet effectivement d'atteindre le but légitime précisé ci-avant. *Secundo*, il semble n'exister aucune autre mesure moins attentatoire pour la liberté d'expression : anonymiser présente le double avantage de laisser l'information en ligne, tout en protégeant adéquatement la vie privée de la personne visée. *Tertio*, la mesure doit être proportionnée au sens strict.

36. L'analyse de la proportionnalité *stricto sensu*. L'analyse de la proportionnalité au sens strict requiert la mise en œuvre d'une balance des intérêts en présence. Pour ce faire, les juridictions belges semblent s'appuyer sur une série de critères mis en lumière dès les premières décisions relatives au « droit à l'oubli » dans la presse traditionnelle (écrite et audiovisuelle)⁸¹, ceux-ci ayant ensuite été systématisés par la doctrine⁸². La liste des critères proposés ressemble, à plusieurs égards, aux éléments qui ont d'ores et déjà été explicités

⁷⁹ Voy. Cour eur. D.H., 9 novembre 2006, *Leempoel & S.A. Éd. Ciné Revue c. Belgique*, req. 64772/09. En revanche, une telle combinaison de dispositions afin de former la norme n'a pas été validée dans le cadre d'une affaire relative à une mesure préventive à l'encontre d'une émission de télévision (Cour eur. D.H., 29 mars 2011, *RTBF c. Belgique*, req. 50084/06).

⁸⁰ À ce propos, la Cour européenne des droits de l'homme admet que la jurisprudence puisse constituer cette norme. Voy. not. Cour eur. D.H., 29 mars 2011, *RTBF c. Belgique*, req. 50084/06. La Cour se penche sur la jurisprudence des juridictions supérieures ainsi que des juridictions de fond pour vérifier s'il existe une tendance claire et unanime dans la validation d'une mesure préventive à l'égard d'une émission de télévision. En l'espèce, elle conclut à l'absence d'une telle tendance et, donc, à l'absence de la prévisibilité requise. Civ. Neufchâteau (2^e ch.), 25 janvier 2013, A.M., 2013/6, p. 478, note ; J.L.M.B., 2013, p. 1182 ; Civ. Bruxelles (4^e ch.), 25 mai 2011, A.M., 2011/4-5, p. 569 ; Civ. Namur (1^{re} ch.), 27 septembre 1999, A.M., 2000/4, p. 471 ; Civ. Namur, 17 novembre 1997, J.L.M.B., 1998, p. 785, note A. STROWEL, « Liberté de rappeler des faits contre droit au silence : les contretemps de la presse » ; Civ. Bruxelles (14^e ch.), 30 juin 1997, J.T., 1997, p. 710.

⁸² Voy. not. A. STROWEL, « Le droit à l'oubli du condamné : après le moment du compte rendu vient le temps du silence », in P. GÉRARD et Fr. OST (dir.), *L'accélération du temps juridique*, Bruxelles, Publications des F.U.S.L., 2000, pp. 742 et s. ; A. STROWEL, « Liberté de rappeler des faits contre droit au silence : les contretemps de la presse », note sous Civ. Namur, 17 novembre 1997, J.L.M.B., 1998, pp. 785 et s.

dans le cadre de la balance des intérêts devant être faite pour mettre en œuvre le droit au déréfèrencement (voy. *supra*, n°s 13-25). En outre, certains d'entre eux se retrouvent, en toute logique, dans la jurisprudence de la Cour européenne des droits de l'homme, plus spécifiquement ses arrêts relatifs au conflit entre la liberté d'expression et la vie privée⁸³. Nous estimons que la liste des critères n'est pas exhaustive, de sorte que de futures décisions en la matière pourraient s'appuyer sur de nouveaux éléments pour évaluer les intérêts en présence, cette approche étant éminemment circonstancielle.

Le premier élément pris en compte est le fait que l'information ait été diffusée licitement une première fois, quelle que soit la forme de cette divulgation (écrit, audiovisuel, Internet). À défaut, le droit à l'information pourrait prévaloir, pour autant évidemment que la diffusion ne soit pas fautive ou que les informations ne soient pas, par exemple, inexactes⁸⁴. Il peut être intéressant de se demander si ce premier élément doit être conçu comme une condition obligatoire ou simplement comme un critère d'appréciation. Cela revient en réalité à s'interroger sur le fait de pouvoir éventuellement invoquer l'anonymisation d'informations face à une unique diffusion qui interviendrait des années après les faits. Cela étant, la question est davantage relative à la pertinence de la divulgation et, donc, à l'éventuelle absence d'un intérêt général des parties.

Un deuxième critère mis en exergue par la jurisprudence concerne l'existence d'une deuxième divulgation. Cette dernière peut intervenir sous n'importe quelle forme, indépendamment du support utilisé pour la première diffusion. Sur Internet, la Cour de cassation, dans son arrêt du 29 avril 2016, a validé le principe selon lequel « l'archivage en ligne de l'article litigieux constitue une nouvelle divulgation du passé judiciaire du défendeur pouvant porter atteinte à son droit à l'oubli ». En réalité, elle reprend ici une partie du raisonnement que les juges européens ont tenu dans l'arrêt *Google Spain*⁸⁵. Nous avons à ce propos écrit que la rediffusion se déduit « de l'effet de l'outil de recherche qui met "en une" une information qui, sinon, serait invisible sur la toile »⁸⁶.

⁸³ Voy. not. Cour eur. D.H. (gde ch.), 7 février 2012, *von Hannover c. Allemagne* (n° 2), req. 40660/08 et 60641/08; Cour eur. D.H. (gde ch.), 7 février 2012, *Axel Springer c. Allemagne*, req. 39954/08.

⁸⁴ Cela rejoint les obligations relatives à la qualité des données établies par la réglementation relative à la protection des données à caractère personnel.

⁸⁵ À ce propos, tout en reconnaissant que les faits ne sont pas exactement identiques, puisque l'arrêt européen oppose un citoyen à un moteur de recherche (et non pas à un éditeur), la Cour d'appel de Liège, dans son arrêt précité du 25 septembre 2014, a consenti à transposer les enseignements de l'arrêt européen « dans la mesure où l'éditeur permet également une mise en ligne de l'article litigieux via le moteur de recherche de son site consultable gratuitement, mise en ligne qui est, par ailleurs, multipliée considérablement par le développement des logiciels d'exploitation des moteurs de recherche du type Google ». Un raisonnement tout à fait identique est proposé par le tribunal de première instance dans son jugement du 3 novembre 2014. Cela étant, dans cette dernière décision, le raisonnement apparaît dans le cadre de l'analyse de la réparation du dommage.

⁸⁶ E. CRUYSMANS et A. STROWEL, « Le droit à l'oubli face aux moteurs de recherche : droit applicable et responsabilité pour le référencement de données "inadéquates, non pertinentes ou excessives" », *op. cit.*, p. 458, n° 9.

Cette reprise nous paraît mettre en exergue le fait que la responsabilité de l'éditeur dont il est question dans le cadre des demandes d'anonymisation est liée à l'activité – et donc au traitement de données – des moteurs de recherche. C'est en effet parce qu'un individu requiert de la part d'un moteur de recherche qu'une recherche soit effectuée aboutissant à retrouver « en une » des résultats particuliers qu'il y aurait rediffusion dans le chef de l'éditeur.

L'analyse du troisième critère aboutit à s'interroger sur le champ d'application de cet oubli, matérialisé dans une demande d'anonymisation. La lecture de la jurisprudence belge citée précédemment nous oblige à déduire que le seul passé judiciaire permet de justifier une telle requête. La Cour de cassation elle-même, à plusieurs reprises, fait référence à ce seul type de passé : elle constate que le droit à l'oubli concerne une « personne coupable d'un crime ou d'un délit » lui permettant de s'opposer à ce que « son passé judiciaire soit rappelé ». Il faudrait donc déduire qu'il n'existerait aucune possibilité pour pouvoir exiger la suppression de données personnelles lors de la diffusion d'informations ne relatant pas des affaires judiciaires. Cela étant, la Cour elle-même jette le trouble : reprenant le raisonnement tenu par les conseillers de la Cour d'appel de Liège dans l'arrêt du 25 septembre 2014, elle paraît faire sienne la définition du droit à l'oubli entendu comme « la possibilité pour une personne de demander l'effacement des données qui la concernent, et plus spécialement des données mises en ligne, après une période donnée », tout en ajoutant que « l'enjeu n'est plus d'empêcher ou de sanctionner la mise en lumière de faits anciens mais d'obtenir la suppression d'informations disponibles sur [l]Internet »⁸⁷. Suivant cet état d'esprit, nous suggérons d'étendre l'application de cet oubli en deux étapes. Premièrement, si l'on cantonne l'oubli aux informations judiciaires, il nous paraît devoir être étendu à l'ensemble des parties au procès, en ce compris, par exemple, les victimes. À ce propos, la jurisprudence belge nous donne raison : dans l'affaire ayant abouti à l'arrêt de la Cour de cassation, les faits repris dans l'article se limitent à narrer les circonstances de l'accident, tout en précisant, il est vrai, que le responsable de l'accident avait déjà été vu par un juge d'instruction. Autrement dit ne sont pas seuls visés les articles relatant des condamnations judiciaires, mais bien tout écrit qui explique peu ou prou un élément d'une procédure judiciaire, qu'elle aboutisse ou non à une condamnation. Deuxièmement, si l'on élargit davantage encore le régime de l'oubli, cette dimension « à long terme » du droit à la vie privée doit pouvoir s'appliquer quel que soit le type d'informations visées, pour autant que le juge puisse considérer que la rediffusion implique une atteinte à ce droit. Cette approche nous paraît être plus cohérente, compte tenu du fait que l'oubli se conçoit comme une composante du droit à la vie privée.

⁸⁷ Cette précision révèle peut-être une confusion dans les types de « droit à l'oubli » : en effet, cette définition plus large pourrait en fait viser davantage l'oubli des données à caractère personnel, soumis aux dispositions en la matière, que l'oubli construit sur le fondement de l'article 1382 du Code civil.

L'élément suivant concerne le laps de temps entre les deux divulgations. Dans les critères développés dans le cadre de la mise en balance devant être effectuée pour la protection des données, cet élément temporel est déjà pris en compte (voy. *supra*, n^{os} 17 et 25). Le raisonnement est ici identique. En effet, il faut, pour que la demande d'anonymisation soit accordée, que l'écoulement du temps permette l'oubli. Cette exigence doit être lue parallèlement au critère de l'actualité. En effet, la liberté d'expression et la liberté de la presse doivent prévaloir lorsque l'information à diffuser est justifiée par l'actualité. Cette actualité peut aussi perdurer un certain temps et intéresser l'opinion publique. Cela étant, l'on peut considérer qu'après un certain temps, cet élément d'actualité disparaît, laissant alors place à l'oubli. L'application de ce critère à Internet a amené les juridictions à considérer que le temps pris en compte doit être celui compris « entre la première diffusion de l'article, peu importe son support, et la demande d'anonymisation »⁸⁸. L'adaptation est cohérente au regard de la forme que prend la redivulgaration, à savoir la remise « en une » d'une information dans le cadre d'une recherche. Dans les affaires précitées, les délais ont été considérés comme suffisamment longs : seize années pour l'article diffusé dans *Le Soir*, dix années pour celui publié dans *La Libre Belgique*, et, à nouveau, seize années pour le dernier article paru dans le quotidien *Le Soir*.

Autre élément commun aux deux raisonnements : la prise en compte du caractère public de la personne visée par les informations. Le rôle public que joue un individu entre en considération dans la détermination de l'oubli fondé sur le droit à la vie privée. Nous nous permettons de renvoyer le lecteur aux développements suggérés ci-avant (voy. *supra*, n^o 14).

Le critère suivant concerne l'éventuel intérêt contemporain à la redivulgaration. Il est nécessaire de lier cet élément au critère temporel. Autrement dit, même après un laps de temps, une information pourrait parfaitement conserver un intérêt contemporain, une certaine actualité. L'intérêt public autour de celle-ci est toujours bel et bien existant. Cet intérêt contemporain pose inévitablement la question d'une éventuelle désanonymisation. Imaginons qu'une information devenue sans intérêt soit anonymisée : ne pourrait-elle pas, par la suite, faire l'objet d'une désanonymisation si des circonstances nouvelles ont pour effet de réactiver un intérêt contemporain à sa redivulgaration ?

Dans le même ordre d'idées, l'intérêt historique peut aussi justifier le refus de mise en œuvre d'une anonymisation. L'objectif de ce droit n'est, en effet, pas d'effacer des pans de l'histoire. Dans cette perspective, l'oubli qui justifie l'anonymisation s'oppose souvent à ce que l'on appelle le « devoir de mémoire ». Sans entrer dans de larges développements en la matière, on peut toutefois considérer que ce devoir est essentiellement d'ordre moral, sauf lorsqu'il s'ins-

⁸⁸ Voy. les propos d'E. DEFRYNE et R. ROBERT, « L'arrêt "Google Spain" : une clarification de la responsabilité des moteurs de recherche... aux conséquences encore floues », *op. cit.*, p. 95.

crit dans le cadre des lois mémorielles ainsi que des lois d'imprescriptibilité⁸⁹. À propos de cet intérêt historique, le jugement précité du Tribunal de première instance de Neufchâteau du 25 janvier 2013 soutient que l'argument tiré de l'intérêt historique ne peut être pertinent dès lors que les demandes ne portent pas sur un retrait des articles litigieux, mais simplement sur l'anonymisation des versions électroniques. De sorte que l'accès à ces documents est toujours dou-blement garanti : soit en ligne par une version anonymisée, soit dans les archives papier, en version intégrale. La Cour d'appel de Liège, dans son arrêt précité du 25 septembre 2014, abonde dans un sens identique en considérant que « le fait d'accueillir la demande formulée par l'intimé n'a pas pour effet de conférer à chaque individu un droit subjectif de réécrire l'histoire ni de permettre une "falsification de l'histoire" [...] ».

Enfin, un dernier élément dans cette mise en balance des intérêts concerne l'intérêt à la resocialisation de la personne visée ainsi que l'apurement de sa dette envers la société. Le critère nous semble cependant plus difficile à mettre spécifiquement en œuvre. En effet, l'objectif même d'un « droit à l'oubli » invoqué par une demande en anonymisation est de permettre cette resocialisation. En cela, il s'apparente à une sorte de réhabilitation applicable dans le droit à la vie privée. De même, l'apurement de la dette envers la société semble quasiment constituer un préalable, lorsque l'oubli porte sur des informations judiciaires, pour requérir la suppression de certaines informations personnelles. La jurisprudence évoquée traite d'ailleurs relativement rapidement ce critère.

2. Le lien de causalité et le dommage

37. Lien de causalité et dommage. Outre la faute, l'action en responsabilité civile extracontractuelle requiert la présence d'un lien de causalité ainsi que d'un dommage. En ce qui concerne le lien de causalité, la théorie de l'équivalence des conditions est d'application. Ainsi, la Cour d'appel de Liège, dans son arrêt de 2014, réfute l'argument invoqué par l'éditeur responsable qui soulignait que « le préjudice subi par l'intimé trouverait uniquement sa cause dans les faits infractionnels de 1994 ainsi que dans l'indexation que fait Google des articles du journal *Le Soir* ». Les juges admettent en outre que, si la demande d'anonymisation avait reçu une réponse favorable, « les moteurs de recherche tels que Google ne renseigneraient pas l'existence de l'article litigieux et aucune atteinte quelconque au droit à l'oubli et à la réputation de l'intimé ne serait à déplorer », établissant *in fine* l'existence du lien de causalité.

Enfin, il s'agit généralement essentiellement d'un préjudice moral résultant d'une atteinte à leur droit à la vie privée et à leur réputation. Cela étant, dans l'une des affaires, un préjudice matériel est invoqué compte tenu du fait de l'exercice d'une profession en contact avec du public.

⁸⁹ Cela étant, les lois mémorielles font l'objet d'âpres débats quant à leur légitimité.

38. L'anonymisation comme mode de réparation. La démonstration de l'existence d'une faute, d'un lien de causalité et d'un dommage permet à l'article 1382 du Code civil de sortir ses effets et d'exiger la réparation de la part de l'éditeur du préjudice subi par la personne visée par les informations. Dans les cas d'espèce visés préalablement, les juges ordonnent l'anonymisation des informations, considérant que ce mode de réparation est adéquat pour garantir la protection de la vie privée, tout en assurant la disponibilité du support.

À ceux qui pourraient invoquer la création d'une censure moderne, la Cour d'appel de Liège, dans son arrêt précité de 2014, répond que « le fait d'accueillir la demande formulée par l'intimé n'a pas pour effet de conférer à chaque individu un droit subjectif de réécrire l'histoire ni de permettre une "falsification de l'histoire" ni de créer dans le chef de l'appelant une "responsabilité exorbitante" ». Ainsi, il ne peut être question de censure ou de réécriture de l'histoire : il s'agit simplement de mettre en balance par le biais d'une anonymisation deux droits fondamentaux qui, en théorie, ne sont pas hiérarchisés. L'approche « au cas par cas » est évidemment inévitable, « engendrant nécessairement des décisions divergentes notamment en fonction du fondement juridique choisi et des particularités de l'espèce », ainsi que de la teneur de la demande initiale. En effet, un retrait total des articles en ligne ne devrait que rarement recevoir de réponse positive de la part de la justice. En revanche, l'anonymisation, accompagnée d'une éventuelle désindexation, constitue sans nul doute un bon équilibre permettant de limiter les atteintes à la vie privée, tout en conservant le droit d'accéder à l'information reconnu à l'article 10 de la Convention européenne des droits de l'homme.

Conclusion

39. Vie privée, données personnelles et responsabilité : de nouvelles prérogatives pour de nouvelles problématiques. Face aux nouvelles situations créées par les développements numériques, le droit répond. Il s'adapte par le biais de nouvelles prérogatives prenant pour fondement les dispositions relatives à la protection des données à caractère personnel et/ou le droit au respect de la vie privée. La tâche est complexe : prendre en compte ces droits et les faire cohabiter avec les libertés d'expression et de presse, ainsi que le droit pour le public d'accéder aux informations. L'anonymisation et le déréférencement, qui ont retenu notre attention, constituent des pistes crédibles en vue d'assurer un équilibre entre l'ensemble des droits fondamentaux en présence. Certes, comme le souligne Mélanie Clément-Fontaine, nous sommes conscients que « l'anonymisation, le déréférencement ou le retrait d'un article peuvent sembler anodins à l'échelle de l'humanité » alors même que leur application conduit à « admettre que la mémoire [puisse] être amputée d'informations et,

de ce fait, dévoyée⁹⁰. Cela étant, compte tenu des outils juridiques existants, les droits évoqués nous paraissent remplir leur rôle : certes, ils limitent la liberté d'expression au sens large, mais permettent de protéger le droit à la vie privée. Aucun de ces droits fondamentaux n'est supérieur à l'autre, aucun n'est absolu, et il y a donc lieu d'organiser une solution intermédiaire, solution que l'anonymisation et le déréférencement semblent, dans l'état actuel du droit, satisfaire.

⁹⁰ M. CLÉMENT-FONTAINE, « Faut-il se réjouir de la percée du droit à l'oubli numérique ? », *op. cit.*, p. 454.

Responsabilités et numérique

Les actes illicites commis sur les réseaux ou, plus généralement, au moyen des technologies de l'information et de la communication tendent à se multiplier. On songe par exemple aux propos diffamatoires, discriminatoires ou racistes tenus sur un réseau social, aux violations des droits de propriété intellectuelle réalisées à travers des sites de téléchargement illicites ou des plates-formes de ventes entre particuliers, voire encore aux traitements de données non conformes à la législation applicable, etc. Ces actes sont susceptibles d'engager la responsabilité pénale et/ou civile de leur auteur. Cette responsabilité doit s'apprécier dans un environnement de plus en plus complexe, où l'identification des auteurs est souvent difficile, et dans lequel interviennent des plates-formes d'intermédiation jouant un rôle plus ou moins actif dans la production de contenus.

Le présent ouvrage se penche sur ces questions épineuses et, parfois, peu connues par les praticiens du droit.

Après une analyse transversale des règles classiques de responsabilité civile et pénale, appliquées au numérique, et du régime d'exonération des prestataires intermédiaires, les contributions portent sur certains domaines plus spécifiques, en lien avec la propriété intellectuelle, les droits fondamentaux, en ce compris la protection des données et la responsabilité des robots.

*Sous la coordination scientifique
d'Hervé Jacquemin,
Maureen Degeldre,
Hélène Preumont
et Zoé Trusgnach*

Nathalie Colette-Basecqz
Alexandre Cruquenaire
Edouard Cruysmans
Elise Franco
Hervé Jacquemin
Jean-Benoît Hubin
Élodie Lecroart
Frédéric Lejeune
Alain Strowel
Pierre-Yves Thoumsin

JEUNE BARREAU DE NAMUR

COLLECTION

Responsabilités et numérique

*Sous la coordination scientifique d'Hervé Jacquemin,
Maureen Degeldre, Hélène Preumont et Zoé Trusgnach*

Nathalie Colette-Basecqz
Alexandre Cruquenaire
Edouard Cruysmans
Elise Franco
Hervé Jacquemin
Jean-Benoît Hubin
Élodie Lecroart
Frédéric Lejeune
Alain Strowel
Pierre-Yves Thoumsin



RESNUM
ISBN: 978-2-8072-0398-3
9 782807 203983

