

Paris, le 30 novembre 2017

Décision du Défenseur des droits n° 2017-326

Le Défenseur des droits,

Vu l'article 71-1 de la Constitution du 4 octobre 1958 ;

Vu la loi organique n° 2011-333 du 29 mars 2011 relative au Défenseur des droits ;

Vu le décret n° 2011-904 du 29 juillet 2011 relatif à la procédure applicable devant le Défenseur des droits ;

Vu la Charte des droits fondamentaux de l'Union européenne, notamment ses articles 7 et 8 ;

Vu la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, notamment ses articles 1 et 8 ;

Vu la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Le 20 septembre 2017, en application de l'article 23 du Statut de la Cour de justice de l'Union européenne, le Défenseur des droits a été invité en qualité de partie en cause devant le Conseil d'Etat dans l'affaire n°399922, à déposer des observations écrites sur la demande de décision préjudicielle datant du 19 juillet 2017 (affaire n° C-507/17 L'entreprise X),

Décide de présenter les observations suivantes devant la Cour.

Le Défenseur des droits

Jacques TOUBON

Tierce-intervention du Défenseur des droits devant la Cour de justice de l'Union européenne dans l'affaire préjudicielle « C-507/17 L'entreprise X »

A la suite de l'arrêt de la Cour de justice de l'Union européenne (« la Cour de justice ») du 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*¹ (« arrêt Google Spain ») et de saisines de réclamants, la Commission nationale de l'informatique et des libertés (« la CNIL »), autorité française de protection des données personnelles, a adressé à L'entreprise X plusieurs demandes de déréférencement sur l'ensemble des extensions du nom de domaine de son moteur de recherche.

Le 21 mai 2015, la CNIL a adopté une mise en demeure enjoignant à la société L'entreprise X de procéder auxdits déréférencements sous un délai de 15 jours. Le 30 juillet 2015, la société a exercé un recours gracieux auprès de la CNIL afin d'obtenir le retrait de sa décision. Ce recours a été rejeté. Après avoir engagé une procédure de sanction et recueilli les observations de la société, la CNIL a, par une délibération du 10 mars 2016, prononcé une sanction pécuniaire d'un montant de 100 000 euros à l'encontre de la société. La société a exercé un recours devant le Conseil d'Etat. A la suite de la saisine de la CNIL, le Défenseur des droits a déposé des observations en qualité d'*amicus curiae* devant la juridiction.²

Le 19 juillet 2017, le Conseil d'Etat a décidé de surseoir à statuer sur l'affaire et de saisir la Cour de justice des trois questions préjudicielles suivantes :

« 1° Le « droit au déréférencement » tel qu'il a été consacré par la Cour de justice de l'Union européenne dans son arrêt du 13 mai 2014 sur le fondement des dispositions des articles 12, sous b), et 14, sous a), de la directive du 24 octobre 1995, doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche est tenu, lorsqu'il fait droit à une demande de déréférencement, d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur 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 ?

2° En cas de réponse négative à cette première question, le « droit au déréférencement » tel que consacré par la Cour de justice de l'Union européenne dans son arrêt précité doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche est seulement tenu, lorsqu'il fait droit à une demande de déréférencement, de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur sur le nom de domaine correspondant à l'Etat où la demande est réputée avoir été effectuée ou, plus généralement, sur les noms de domaine du moteur de recherche qui correspondent aux extensions nationales de ce moteur pour l'ensemble des Etats membres de l'Union européenne ?

3° En outre, en complément de l'obligation évoquée au 2°, le « droit au déréférencement » tel que consacré par la Cour de justice de l'Union européenne dans son arrêt précité doit être interprété en ce sens que l'exploitant d'un moteur de recherche faisant droit à une demande de déréférencement est tenu de supprimer, par la technique dite du « géo-blocage », depuis une adresse IP réputée localisée dans l'Etat de résidence du bénéficiaire du « droit au déréférencement », les résultats litigieux des recherches effectuées à partir de son nom, ou même, plus généralement, depuis une adresse IP réputée localisée dans l'un des Etats-membres soumis à la directive du 24 octobre 1995, ce indépendamment du nom de domaine utilisé par l'internaute qui effectue la recherche ? »³

¹ CJUE, *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, 13 mai 2014, C-131/12.

² Décision n° 2016-311, 7 décembre 2016.

³ Conseil d'Etat, 19 juillet 2017, *GOOGLE INC.*, n° 399922.

Le 20 septembre dernier, en application de l'article 23 du statut de la Cour de justice, le Défenseur des droits a été invité en qualité de "partie en cause" devant le Conseil d'Etat dans l'affaire n°399922, à déposer des observations écrites sur la demande de décision préjudicielle datant du 19 juillet 2017 (affaire C-507/17 L'entreprise X).

Les observations du Défenseur des droits sont présentées ci-dessous.

I. Le droit au respect de la vie privée et à la protection des données personnelles : un droit fondamental

La Charte des droits fondamentaux de l'Union européenne (« la Charte ») garantit le droit au respect de la vie privée et la protection des données à caractère personnel, respectivement à ses articles 7 et 8. L'article 8 dispose en outre que ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Il prévoit également que tout individu a le droit d'accéder aux données collectées le concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

Ces droits ainsi que le principe d'une protection élevée des données à caractère personnel sont inscrits dans la Directive 95/46/CE du Parlement européen du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (« la Directive 95/46/CE »). Ses articles 12 et 14 garantissent en effet des droits d'accès et d'opposition et imposent aux Etats membres de garantir à toute personne concernée :

- le droit d'obtenir du responsable du traitement de données personnelles la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données ;
- le droit de s'opposer, dans certains cas visés par la directive, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national.

La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, qui fait partie du droit de l'Union,⁴ protège, elle aussi, les données personnelles au titre de l'article 8 sur le droit au respect de la vie privée. La Cour européenne des droits de l'homme (« CEDH ») l'a notamment rappelé dans l'arrêt *S. et Marper c. Royaume-Uni* : « *La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention* ». ⁵ Ce droit est également garanti par la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981.

II. La reconnaissance d'un « droit au déréférencement » par la Cour de justice et d'une responsabilité des exploitants de moteurs de recherche

Interrogée dans le cadre d'un recours préjudiciel sur l'interprétation à donner à la Directive 95/46/CE, la Cour de justice a consacré implicitement, dans l'arrêt *Google Spain* du 13 mai 2014, « un droit au déréférencement », au titre des articles 12 et 14 de la Directive et des articles 7 et 8 de la Charte. Elle a en effet statué comme suit : « *88 (...) les articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46 doivent être interprétés en ce sens que, afin de respecter les droits prévus à ces dispositions et pour autant que les conditions prévues par celles-ci sont effectivement satisfaites, l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom*

⁴ Article 6§3 du Traité sur l'Union européenne.

⁵ CEDH, *S. et Marper c. Royaume-Uni*, 4 décembre 2008, § 103.

d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite [accent ajouté]. »

La Cour justifie la reconnaissance de ce droit au déréférencement comme suit : « 80 (...) un traitement de données à caractère personnel, tel que celui en cause au principal, réalisé par l'exploitant d'un moteur de recherche, est susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel lorsque la recherche à l'aide de ce moteur est effectuée à partir du nom d'une personne physique, dès lors que ledit traitement permet à tout internaute d'obtenir par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet, qui touchent potentiellement à une multitude d'aspects de sa vie privée et qui, sans ledit moteur de recherche, n'auraient pas ou seulement que très difficilement pu être interconnectées, et ainsi d'établir un profil plus ou moins détaillé de celle-ci. En outre, l'effet de l'ingérence dans lesdits droits de la personne concernée se trouve démultiplié en raison du rôle important que jouent Internet et les moteurs de recherche dans la société moderne, lesquels confèrent aux informations contenues dans une telle liste de résultats un caractère ubiquitaire. »

En consacrant le droit au déréférencement, la Cour de justice permet ainsi aux individus d'avoir la pleine maîtrise de leurs données personnelles sur Internet.⁶ La Cour de Strasbourg reconnaît également ce droit sous la forme d'un « droit à une forme d'autodétermination informationnelle », qui permet à un individu d'invoquer le droit au respect de la vie privée concernant des données qui sont collectées, traitées et diffusées à la collectivité, selon des formes ou modalités telles que ses droits au titre de l'article 8 peuvent être mis en jeu.⁷ Le droit à l'autodétermination informationnelle est un concept qui a été dégagé en 1983 par la Cour constitutionnelle allemande ; celle-ci considère que ce droit est attaché à la personne et lie la protection des données personnelles aux droits constitutionnels de la personne à la dignité humaine et au libre développement de sa personnalité.⁸

Le droit au déréférencement serait une forme de droit à l'oubli numérique, « un droit dérivé » des droits d'accès, à la rectification et à l'effacement des articles 12 et 14 de la Directive 95/46/CE. Il est désormais inscrit dans le nouveau règlement général 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (« RGPD »)⁹ qui entrera en vigueur le 25 mai 2018, sous l'intitulé « droit à l'effacement (« droit à l'oubli ») ».

De ce droit au déréférencement résultent des obligations pour les exploitants de moteurs de recherche sur Internet soumis à législation européenne. Dans l'arrêt *Google Spain*, la Cour de justice considère qu'en recherchant de manière automatisée, constante et systématique des informations publiées sur Internet, l'exploitant d'un moteur de recherche procède à une « collecte » des données 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 ; ces opérations constituent donc un « traitement » au sens de la directive 95/46/CE (article 2).¹⁰

⁶ Conseil d'Etat, Etude « *Le numérique et les droits fondamentaux* » de 2014, p.184.

⁷ CEDH, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], no 931/13, § 137 ; voir également Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, L'autodétermination informationnelle à l'ère d'Internet, T-PD (2004) 04.

⁸ BVerfG, jugement, 15 décembre 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1.

⁹ Règlement (UE) 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.

¹⁰ CJUE, arrêt *Google Spain*, §§ 28, 41.

La Cour juge par ailleurs que l'exploitant du moteur de recherche est le « responsable » de ce traitement, au sens de la directive, étant donné que c'est lui qui en détermine les finalités et les moyens.¹¹ Le fait que ce dernier n'exerce aucun contrôle sur les données personnelles publiées sur les pages web des tiers ne saurait l'exonérer de cette responsabilité.¹² Concernant le champ d'application de la directive, la Cour observe que *Google Spain* constitue une filiale de Google Inc. sur le territoire espagnol et, partant, un « établissement » au sens de la directive.

Dès lors, l'exploitant du moteur de recherche doit se conformer au droit européen et respecter les droits protégés par la Directive et la Charte, y compris le droit au déréférencement, lorsque les conditions sont satisfaites.¹³

III. Le droit au déréférencement : un droit qui n'est ni automatique, ni absolu

A titre préliminaire, il convient de rappeler que le droit au déréférencement consacré par la Cour de justice ne consiste pas à supprimer le contenu de l'information d'Internet mais à « *supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne* ». ¹⁴ En effet, le contenu original de l'information reste inchangé et demeure accessible via les moteurs de recherche en utilisant des mots clés ou en allant directement sur le site internet à l'origine de la diffusion de l'information.¹⁵ Alléguer que le droit au déréférencement conduirait à une censure sur Internet et une atteinte disproportionnée à la liberté d'expression et d'accès à l'information serait donc excessif. C'est d'ailleurs ce que souligne le Commissaire aux droits de l'homme du Conseil de l'Europe, Nils Muižnieks, dans un rapport de 2014, intitulé « *La prééminence du droit sur l'internet et dans le monde numérique en général* ». Selon lui, le déréférencement imposé à Google a un impact très réduit sur l'accès à l'information en ligne : « *In that way, the obligation placed on Google has the smallest possible effect on freedom of communication online while achieving the clearly proportionate goal of removing unfair and prejudicial search results, when these are based on an individual's name.* »¹⁶

Ensuite, la demande de déréférencement ne peut être accueillie que si elle remplit certaines conditions.¹⁷ Celles-ci sont inscrites dans la Directive 95/46/CE et ont été rappelées par la Cour de justice dans l'arrêt *Google Spain*. La demande peut être accueillie si n'ont pas été respectés les principes relatifs à la qualité des données fixés à l'article 6 de la Directive (les données sont inexactes, inadéquates non pertinentes ou excessives au regard des finalités du traitement, ou conservées pendant une durée excédant celle nécessaire) et à la légitimation des traitements de données fixés à l'article 7. La Cour de justice précise par ailleurs que le déréférencement peut être demandé alors même que la publication des données personnelles est licite et que l'inclusion de l'information dans la liste des résultats du moteur de recherche ne cause aucun préjudice à la personne. Consciente des difficultés rencontrées pour démontrer l'existence d'un préjudice, la Cour a décidé de ne pas exiger cette condition.¹⁸

Par ailleurs, le déréférencement peut être refusé dans certaines situations, notamment lorsque la conservation des données personnelles s'impose à des fins historiques, statistiques ou scientifiques.

¹¹ *Ibid.*

¹² CJUE, arrêt *Google Spain*, § 34.

¹³ *Ibid.*, § 89.

¹⁴ CJUE, arrêt *Google Spain*, § 82.

¹⁵ Voir par exemple CNIL, Le droit au déréférencement ; A. Strowel, Le « droit à l'oubli » : mal nommé, mal défini, mais bienvenu ; A propos de l'arrêt Google de la Cour de justice, 2014.

¹⁶ Commissaire aux droits de l'homme du Conseil de l'Europe, La prééminence du droit sur l'internet et dans le monde numérique en général, 2014.

¹⁷ CJUE, arrêt *Google Spain*, § 88 « *et pour autant que les conditions prévues par [les dispositions des articles 12 et 14] sont effectivement satisfaites...* ».

¹⁸ I. Gheorghe-Bădescu, Le droit à l'oubli numérique, De l'Europe au Japon, Revue de l'Union européenne, 2017 p.153.

Si la Cour de justice estime que la gravité potentielle de l'ingérence de l'activité du moteur de recherche dans les droits de la personne concernée ne saurait être justifiée par le seul intérêt économique de l'exploitant d'un tel moteur dans ce traitement, elle considère cependant que la suppression de liens de la liste de résultats par la voie du déréférencement pourrait « *en fonction de l'information en cause, avoir des répercussions sur l'intérêt légitime des internautes potentiellement intéressés à avoir accès à celle-ci* ». Dès lors, toute demande de déréférencement doit donner lieu à la recherche d'un juste équilibre entre notamment cet intérêt et les droits fondamentaux de cette personne au titre des articles 7 et 8 de la Charte.

Tout en donnant une prééminence aux droits de la personne invoquant la protection de ses données personnelles, la Cour indique que cette mise en balance des droits et intérêts opposés doit tenir compte de la nature de l'information référencée, de la date de la publication initiale des données, de la sensibilité pour la vie privée de la personne concernée et des circonstances entourant la situation concrète de cette personne, ainsi que de l'intérêt public à disposer de cette information, celui-ci pouvant varier, notamment, en fonction du rôle joué par cette personne dans la vie publique.¹⁹

Bien que la Cour de justice n'ait pas fait explicitement référence à la jurisprudence de la CEDH, sa position dans l'arrêt *Google Spain* semble bien aller dans même le sens : la recherche d'un juste équilibre entre le droit au respect de la vie privée et la liberté d'expression, qui garantit non seulement le droit de communiquer des informations mais également celui, pour le public, d'en recevoir²⁰.

Le bien-fondé de chaque demande de déréférencement devra être attentivement examiné en procédant à cette mise en balance des droits et des intérêts en cause, à la lumière des critères fixés par la Cour de justice et la CEDH. Ce qui peut sembler toutefois discutable, c'est que cet examen soit effectué par l'exploitant du moteur de recherche saisi de la demande de déréférencement, alors que celui-ci est une entreprise privée, « à la fois juge et partie », et qu'en principe, l'obligation de protection des données personnelles inscrite dans la Directive incombe aux autorités publiques (notamment au juge).²¹ Le fait qu'en cas de désaccord avec le responsable du traitement, l'autorité nationale de protection des données et/ou le juge national puissent être saisis *a posteriori* par le requérant et opérer le contrôle de nécessité et de proportionnalité requis, serait-il suffisant à compenser cette faille ? On peut s'interroger. Par ailleurs, cette situation pourrait créer une insécurité juridique, les critères concrets d'examen des demandes de déréférencement pouvant varier selon les exploitants des moteurs de recherche.

Il convient également de constater qu'il ressort du rapport de Google Transparency et du nombre élevé de demandes de déréférencement que le droit au déréférencement répond à un besoin social et juridique.²² En France, en 2016, la CNIL a reçu plus de 400 demandes de déréférencement, soit plus de 1 000 demandes depuis mai 2014. Cependant, dans le même temps, il faut souligner que l'examen de chaque demande n'aboutit pas nécessairement à une réponse favorable. La majorité de ces demandes fait l'objet d'un rejet ; à titre d'exemple, depuis mai 2014, Google a rejeté 51,4 % des demandes (204 674).

Enfin, le déréférencement n'est ouvert qu'aux personnes se trouvant sur le territoire de l'Union européenne. La Cour de justice a interprété l'article 4 de la Directive comme suit : « (...) *que*

¹⁹ CJUE, *Google Spain*, §§ 76, 81, 97-98.

²⁰ CEDH, *Observer et Guardian c. Royaume-Uni*, 26 novembre 1991, § 59 b.

²¹ Voir, par exemple, A. Cassart, J.-F. Henrotte, Arrêt *Google Spain* : la révélation d'un droit à l'effacement plutôt que la création d'un droit à l'oubli, *Jurisprudence de Liège*, 2014/25 ; A. Strowel, Le « droit à l'oubli » : mal nommé, mal défini, mais bienvenu ; A propos de l'arrêt *Google* de la Cour de justice, 2014. Voir également Conseil d'Etat, *Etude annuelle de 2014, Le numérique et les droits fondamentaux*, p.189.

²² https://transparencyreport.google.com/eu-privacy/overview?privacy_requests=&lu=delisted_urls&delisted_urls=start:1401235200000:end:1508889600000:country:FR; O. Tambou, *Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déréférencement*, HAL, 2017.

l'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre [accent ajouté]. »²³

L'arrêt *Google Spain* constitue une avancée indéniable en matière de protection des données personnelles dans l'ère numérique, cependant plusieurs questions demeurent sur la mise en œuvre concrète de ce droit et sa portée. Elles font précisément l'objet des questions préjudicielles du Conseil d'Etat.

IV. Assurer l'effectivité du « droit au déréférencement » : un enjeu pour la protection des données personnelles

L'effectivité du droit au déréférencement consacré par la Cour de justice dépendra des modalités concrètes de mise en œuvre de ce droit, et en particulier de sa portée territoriale. La Cour ne s'est pas prononcée à ce sujet dans l'arrêt *Google Spain*.

Mesurant les enjeux d'une telle question, le Conseil d'Etat a saisi la Cour de justice de trois questions préjudicielles sur la manière dont doit être concrètement mis en œuvre le déréférencement : 1° doit-il être global, ce qui signifierait que l'exploitant d'un moteur de recherche devrait supprimer les liens litigieux des résultats sur l'ensemble de ses extensions locales ? ; ou 2° doit-il s'appliquer aux extensions nationales du moteur de recherche pour l'ensemble des Etats membres de l'Union européenne ? ; ou encore 3° en complément de la seconde technique, doit-il adapter les résultats de la recherche à l'origine géographique de la requête et supprimer les liens litigieux des résultats lorsque cette requête provient d'une adresse IP réputée localisée dans l'Etat de résidence du bénéficiaire du droit au déréférencement ou d'une adresse IP réputée localisée dans l'un des Etats membres de l'Union européenne ?

Devant le Conseil d'Etat, le rapporteur public soulignait l'ampleur de la problématique centrale du litige à laquelle la Cour de justice doit répondre : celle de l'adaptation des matrices juridiques traditionnelles, reposant sur une forte territorialisation du droit, à l'univers dématérialisé du numérique.²⁴

La décision de la Cour sera donc déterminante.

Aucune disposition de la Directive 95/46/CE ne vient limiter la portée des droits qui y sont consacrés. Au contraire, à la lecture des objectifs poursuivis par la Directive et de l'arrêt *Google Spain*, il semble bien qu'on tende vers la reconnaissance d'un droit au déréférencement d'une portée territoriale telle, qu'elle puisse permettre d'assurer l'effectivité d'une protection efficace et complète des données à caractère personnel. En effet, la Cour a rappelé à plusieurs reprises, dans *Google Spain*, l'objectif poursuivi par la Directive :

« 34 Par ailleurs, il convient de constater qu'il serait contraire non seulement au libellé clair mais également à l'objectif de cette disposition, consistant à assurer, par une définition large de la notion de « responsable », une protection efficace et complète des personnes concernées, d'exclure de celle-ci l'exploitant d'un moteur de recherche au motif qu'il n'exerce pas de contrôle sur les données à caractère personnel publiées sur les pages web de tiers.

(...) 38 Dans la mesure où l'activité d'un moteur de recherche est donc susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites web les

²³ CJUE, arrêt *Google Spain*, § 60.

²⁴ Conclusions, A. Bretonneau, affaire n° 399922 Google Inc.

droits fondamentaux de la vie privée et de la protection des données à caractère personnel, l'exploitant de ce moteur en tant que personne déterminant les finalités et les moyens de cette activité doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que celle-ci satisfait aux exigences de la directive 95/46 pour que les garanties prévues par celle-ci puissent développer leur plein effet et qu'une protection efficace et complète des personnes concernées, notamment de leur droit au respect de leur vie privée, puisse effectivement être réalisée. »

(...) 53 En outre, au vu de l'objectif de la directive 95/46 d'assurer une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée, à l'égard du traitement des données à caractère personnel (...).

(...) 58 Dans ces conditions, il ne saurait être accepté que le traitement de données à caractère personnel effectué pour les besoins du fonctionnement dudit moteur de recherche soit soustrait aux obligations et aux garanties prévues par la directive 95/46, ce qui porterait atteinte à l'effet utile de celle-ci et à la protection efficace et complète des libertés et des droits fondamentaux des personnes physiques qu'elle vise à assurer (voir, par analogie, arrêt L'Oréal e.a., EU:C:2011:474, points 62 et 63), notamment celui au respect de leur vie privée, à l'égard du traitement des données à caractère personnel, auquel cette directive accorde une importance particulière ainsi que le confirment notamment son article 1er, paragraphe 1, et ses considérants 2 et 10 (...).

(...) 66 À titre liminaire, il convient de rappeler que, ainsi qu'il résulte de son article 1er et de son considérant 10, la directive 95/46 vise à garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel (...) [accents ajoutés]. »

A aucun moment dans l'arrêt *Google Spain*, la Cour de justice n'a limité la portée territoriale du droit au déréférencement : « *La personne concernée pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander à ce que l'information en question ne soit plus mise à la disposition du grand public par son inclusion dans une telle liste de résultats* (...) [accent ajouté] ».

L'effectivité des droits protégés par la Directive 95/46/CE et la Charte est une préoccupation commune aux instances de l'Union européenne et du Conseil de l'Europe.

Bien qu'à l'heure actuelle, il ne semble pas y avoir de large consensus en Europe sur la question de la portée du droit au déréférencement, plusieurs arguments militent en faveur d'un déréférencement global, qui serait plus adapté au caractère transnational du traitement de données personnelles opéré par les moteurs de recherche et qui répondrait à l'objectif de protection élevée poursuivi par la Directive 95/46/CE.

C'est la position de la CNIL et du Groupe de travail « Article 29 » (le G29), l'organe consultatif indépendant sur la protection des données et la vie privée, institué au titre de l'article 29 de la Directive 95/46/CE, et qui est composé de représentants des autorités nationales de l'Union compétentes en matière de protection des données, du Contrôleur européen de la protection des données et de la Commission européenne. Dans ses lignes directrices sur la mise en œuvre de l'arrêt *Google Spain*, le G29 indiquait « *In order to give full effect to the data subject's rights as defined in the Court's ruling, de-listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.* ». Le G29 précisait que le bénéfice du droit au déréférencement était limité aux situations où il y a un lien clair entre le réclamant et l'Union européenne, par exemple, lorsque

le réclamant est un citoyen ou un résident d'un Etat membre de l'Union.²⁵ Cette position semble partagée par le Vice-Président pour le Marché unique numérique à la Commission européenne.²⁶

En 2016, l'Association francophone des autorités de protection des données personnelles adoptait une résolution appelant à la reconnaissance d'un droit à l'effacement et au déréférencement de portée universelle.²⁷

Cela semble également être la position du Conseil d'Etat qui a saisi la Cour de justice. Dans son étude annuelle de 2014 portant sur le numérique et les droits fondamentaux, il estime que pour que la mise en œuvre du droit au déréférencement soit efficace, le déréférencement doit concerner l'ensemble des versions nationales d'un même moteur de recherche (pour Google, les versions nationales mais aussi Google.com).²⁸

L'effectivité du droit au déréférencement s'inscrit dans la logique du Traité sur le fonctionnement de l'Union européenne (article 16), de la Directive 95/46/CE et de la Charte qui garantit à toute personne, en son article 8, ce droit fondamental qu'est la protection de ses données personnelles.

La protection des données personnelles est en effet consacrée en droit de l'Union européenne comme un droit fondamental majeur²⁹, attaché à la personne, dont peut se prévaloir tout individu se trouvant sur le territoire de l'Union européenne, à partir du moment où celui-ci fait l'objet d'un traitement de données à caractère personnel. Ni la Directive précitée, ni la Charte n'ont entendu limiter la portée de cette protection au territoire de l'Union européenne. Au contraire, il semble bien que la volonté soit de protéger ces données personnelles sans discontinuité, au-delà des frontières, et de garantir l'universalité de cette protection dans une ère dématérialisée et déterritorialisée, où les données personnelles font l'objet de traitements par différentes entités privées et publiques et de transferts d'un pays à l'autre, à des fins diverses.

Cette volonté se manifeste notamment à travers l'instauration d'un régime juridique pour les transferts des données personnelles vers des pays tiers. La Directive 95/46/CE régit en son chapitre IV les transferts de données à caractère personnel vers des pays tiers, en fixant certaines exigences telles que l'existence dans le pays tiers d'un niveau de protection adéquat (articles 25 et 26). Dans l'arrêt *Schrems* du 6 octobre 2015, la Cour de justice rappelait que « l'article 25 de la Directive met en œuvre l'obligation explicite de protection des données à caractère personnel, prévue à l'article 8 de la Charte, et vise à assurer, la continuité du niveau élevé de cette protection en cas de transfert de données à caractère personnel vers un pays tiers [accent ajouté] ». La volonté est bien de garantir que ce niveau élevé de protection des données personnelles ne soit pas contourné et qu'il soit assuré en dehors de l'Union européenne. Selon le Comité consultatif de la Convention du Conseil de l'Europe du 28 janvier 1981, la Directive 95/46/CE consacre bien un régime juridique des flux transfrontières de données présentant un effet extraterritorial.³⁰ Ce que constate également le Conseil d'Etat dans son rapport sur le numérique de 2014.

Afin d'atteindre les objectifs poursuivis par la Directive 95/46/CE, de telles dispositions doivent nécessairement empiéter sur la souveraineté des Etats tiers : « *The duty to safeguard the fundamental rights of the Union's citizens does not end at the frontiers of the Union. On the*

²⁵ G29, Guidelines on the implementation of the Court of justice of the European Union Judgment on "Google Spain and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González", C-131/12, pts 6 et 7.

²⁶ <https://gigaom.com/2015/02/12/eu-privacy-rulings-should-apply-globally-says-digital-chief/>.

²⁷ CNIL, rapport d'activité, 2016.

²⁸ Conseil d'Etat, Etude annuelle de 2014, Le numérique et les droits fondamentaux, p.277.

²⁹ CJUE, *Maximilian Schrems contre Data Protection Commissioner*, 6 octobre 2015, C-362/14.

³⁰ DG I – Droits de l'Homme et État de droit, Note relative à l'introduction du concept de juridiction dans l'article 1^{er} de la Convention n° 108, 5 septembre 2012.

contrary, the Union is no less bound to achieve a high degree of protection for all transborder flows of data (...) Simply, the Internet is a global network. By seeking to regulate an international medium, the E.U. necessarily must unilaterally impose its will upon the medium as a whole - it cannot simply regulate that portion of the Internet which exists within its physical territory since data transfers do not recognize boundaries established in the bricks and mortar world. Regardless of the blurred lines demarcating a state's sovereign interests, the Directive's scope necessarily extends beyond the E.U.'s defined territorial boundaries. Therefore, to ensure the maximum protection of privacy, as warranted by what the E.U. perceives to be a fundamental right, it must prescribe and enforce the Directive's protectionary measures wherever the Internet extends. [accent ajouté] ».³¹

En consacrant la protection des données personnelles comme un droit individuel fondamental au sein de l'Union européenne et la garantie d'une protection effective élevée, le législateur européen impose nécessairement aux instances de l'Union et aux Etats membres les obligations associées à ce droit, principalement celles tenant à ne pas s'ingérer de manière arbitraire dans l'exercice de ce droit mais également celles imposant de prendre des mesures tendant à rendre ce droit effectif. Pour donner une pleine effectivité à ce droit, ces obligations peuvent donner des effets extraterritoriaux aux textes européens lorsque l'ingérence est susceptible d'entraîner des répercussions sur ce droit en dehors de la juridiction de l'Etat.

Bien que le déréférencement global puisse poser question au regard des principes de droit international de territorialité et de souveraineté des Etats tiers à l'Union européenne et des risques de conflits de normes,³² ces effets extraterritoriaux sont admis en droit européen.

L'obligation des autorités de prendre des mesures rendant le droit à la protection des données personnelles effectif

La Cour de justice rappelle que les dispositions de la Directive 95/46/CE doivent être interprétées à la lumière des droits fondamentaux garantis par la Charte mais également par la Convention européenne des droits de l'homme.³³

L'article 1 de la Convention européenne dispose que les Etats contractants reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis dans la Convention. Comme indiqué plus haut, le droit au respect de la vie privée protégé par l'article 8 de la Convention inclut la protection des données personnelles.³⁴

Les Etats parties à la Convention européenne ont des obligations en matière de protection de la vie privée et des données personnelles à l'égard des personnes qui relèvent de leur juridiction. Dans un arrêt récent, *Bărbulescu c. Roumanie*, la CEDH a rappelé les obligations des Etats résultant de l'article 8 de la Convention : « *Si l'article 8 (...) a essentiellement pour objet de prémunir l'individu contre des ingérences arbitraires des pouvoirs publics des pouvoirs publics, il peut également imposer à l'Etat des obligations positives inhérentes à un respect effectif des droits qu'il garantit* ». ³⁵ Par ailleurs, avec l'effet horizontal de la Convention, la responsabilité de l'Etat peut être engagée en cas d'ingérence dans le droit au respect de la vie privée d'un individu par une entité privée lorsque les faits résultent d'un manquement de sa part à garantir la jouissance de ce droit.³⁶ A titre d'exemple, dans l'affaire précitée, il s'agissait d'une mesure de surveillance de communications électroniques du requérant par son employeur privé, qui entraîna son licenciement.

³¹ Voir, par exemple, J. S. Bauchner, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, Brooklyn Journal of International Law, 12-1-2000.

³² B. van Alsenoy et M. Koekoek, *The extra-territorial reach of the EU's "right to be forgotten"*, Ku Leuven Center for IT & IP Law, 2015.

³³ CEDH, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], no 931/13, § 70, CEDH 2017.

³⁴ CEDH, *Amann c. Suisse* [GC], no 27798/95, §§ 65 et s, CEDH 2000-II.

³⁵ CEDH, *Bărbulescu c. Roumanie* [GC], no 61496/08, § 108, CEDH 2017.

³⁶ J. Kokott, C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, International Data Privacy Law, 2013.

Les effets extraterritoriaux de la Convention et de la Charte admis en droit européen

Pour donner une pleine effectivité aux droits protégés par la Convention, la Cour européenne a déjà considéré que les obligations des Etats membres peuvent donner des effets extraterritoriaux à la Convention lorsque l'ingérence est susceptible d'entraîner des répercussions sur ce droit en dehors de leur juridiction.

Dans l'affaire *Soering*, par exemple, où il s'agissait de l'extradition d'un individu vers un Etat tiers, les Etats-Unis d'Amérique, qui risquait de s'y voir condamner à la peine capitale, bien que la Cour ait reconnu que la Convention ne régit pas les actes d'un Etat tiers, ni ne prétend exiger des Parties contractantes qu'elles imposent ses normes à cet Etat, elle a néanmoins rappelé que l'objet et le but de la Convention appellent à comprendre et appliquer ses dispositions d'une manière qui en rende ses exigences concrètes et effectives :

« En l'espèce, nul ne le conteste, les pratiques et mesures des autorités virginiennes dont se plaint le requérant échappent au contrôle du Royaume-Uni. Il est aussi exact que d'autres instruments internationaux mentionnés par le gouvernement britannique abordent en termes exprès et précis les problèmes liés à la remise d'une personne à un Etat sur le territoire duquel peuvent s'ensuivre des conséquences non souhaitées, par exemple la Convention des Nations Unies relative au statut des réfugiés, de 1951 (article 33), la Convention européenne d'extradition de 1957 (article 11) et la Convention des Nations Unies, de 1984, contre la torture et autres peines ou traitements cruels, inhumains ou dégradants (article 3). Ces considérations ne sauraient pourtant relever les États contractants de leur responsabilité, au regard de l'article 3 (art. 3), pour tout ou partie des conséquences prévisibles qu'une extradition entraîne en dehors de leur juridiction.

*87. La Convention doit se lire en fonction de son caractère spécifique de traité de garantie collective des droits de l'homme et des libertés fondamentales (arrêt *Irlande contre Royaume-Uni* du 18 janvier 1978, série A no 25, p. 90, § 239). L'objet et le but de cet instrument de protection des êtres humains appellent à comprendre et appliquer ses dispositions d'une manière qui en rende les exigences concrètes et effectives (voir, entre autres, l'arrêt *Artico* du 13 mai 1980, série A no 37, p. 16, § 33). En outre, toute interprétation des droits et libertés énumérés doit se concilier avec "l'esprit général [de la Convention], destinée à sauvegarder et promouvoir les idéaux et valeurs d'une société démocratique" (arrêt *Kjeldsen, Busk Madsen et Pedersen* du 7 décembre 1976, série A no 23, p. 27, § 53). [accents ajoutés] »*

Ainsi, en matière d'éloignement de ressortissants étrangers vers un Etat tiers (extradition ou expulsion), la Cour considère que pour garantir toute l'effectivité à la prohibition absolue de la torture et des traitements inhumains ou dégradants consacrée à l'article 3 de la Convention, l'Etat contractant a l'obligation de vérifier s'il existe des motifs sérieux et avérés de croire que la personne visée par la mesure court un risque réel d'être soumise à un tel traitement, si elle est livrée à l'Etat requérant, et si c'est le cas, de ne pas procéder à son extradition. Pour la Cour, la circonstance que ce traitement soit le fait d'un Etat tiers à la Convention n'entre pas en considération.³⁷

Cette responsabilité peut également se poser sur le terrain des articles 2 (droit à la vie) et 1 du Protocole n° 6 (abolition de la peine de mort)³⁸ mais également de l'article 6 de la Convention - qui protège le droit à un procès équitable - lorsque la personne risque de subir un déni de justice flagrant en cas de transfert vers l'Etat tiers.

S'appuyant sur la jurisprudence de la CEDH, la Cour de justice a dégagé les mêmes obligations, et ce en application de l'article 1^{er} de la Charte, de son article 4 qui interdit de

³⁷ CEDH, *Trabelsi c. Belgique*, no 140/10, CEDH 2014.

³⁸ CEDH, *Jabari c. Turquie*, no 40035/98, CEDH 2000-VIII ; voir, par exemple, *S.R. c. Suède* (déc.), no 62806/00, 23 avril 2002 ; *Ismaili c. Allemagne* (déc.), no 58128/00, 15 mars 2001, et *Bahaddar c. Pays-Bas*, arrêt du 19 février 1998, Recueil 1998-I, avis de la Commission, pp. 270-271, §§ 75-78.

manière absolue la torture et les peines ou traitements inhumains ou dégradants, et de son article 19 qui prévoit une protection absolue contre l'éloignement, l'expulsion ou l'extradition vers un Etat, où il existe un risque sérieux d'être soumis à la peine de mort, à la torture ou à d'autres peines ou traitements inhumains ou dégradants.³⁹

La Cour de justice pourrait transposer ce raisonnement dans la présente affaire. La protection des données personnelles étant un droit fondamental au regard de la Directive 95/46/CE, de la Charte et de la Convention européenne des droits de l'homme, ces textes doivent être appliqués de manière à ce que leurs exigences soient rendues concrètes et effectives. Dès lors, les obligations de l'Etat doivent comprendre l'adoption de mesures visant à garantir que le droit au déréférencement soit pleinement respecté et mis en œuvre ; ce qui donnera nécessairement des effets extraterritoriaux aux textes consacrant le droit au déréférencement, où il y a des éléments d'extranéité, tels que les flux transfrontaliers des données sur Internet, opérés, entre autres, par les exploitants de moteurs de recherche.

En outre, ainsi que le soutient la CNIL, l'unicité du traitement du moteur de recherche milite également en faveur d'une application du déréférencement à l'ensemble du traitement, quels que soient les chemins d'accès transfrontaliers créés. C'est aussi l'avis du rapporteur public devant le Conseil d'Etat.⁴⁰ Comme la CNIL le soutient, il suffirait d'invoquer le caractère transnational d'un traitement pour contourner la protection prévue par le droit européen ; or, c'est bien ce que la Directive 95/46/CE a entendu éviter. A cet égard, l'arrêt *Google Spain* le rappelle : « 54. Il convient de relever dans ce contexte qu'il ressort notamment des considérants 18 à 20 et de l'article 4 de la directive 95/46 que le législateur de l'Union a entendu éviter qu'une personne soit exclue de la protection garantie par celle-ci et que cette protection soit contournée (...). »

Par ailleurs, le fait de faire varier les effets du droit au déréférencement selon les extensions locales du moteur de recherche ou de les limiter au territoire de l'Union européenne nuirait à l'effectivité de ce droit et pourrait ainsi le vider de sa substance. Prenons l'hypothèse suivante : un individu qui obtient, en application du droit européen, le droit au déréférencement à l'égard du moteur de recherche, L'entreprise X, et ce dernier refuse qu'il puisse s'en prévaloir sur les extensions qui se trouvent en dehors de la zone de l'Union européenne, au motif que le droit européen ne serait pas applicable. On peut d'emblée imaginer les difficultés auxquelles cet individu va être confronté pour faire valoir son droit au déréférencement, si, comme le soutiendrait L'entreprise X, il existe autant de traitements liés au service L'entreprise X que d'extensions locales du moteur de recherche : l'impossibilité de se prévaloir de son droit au déréférencement en raison de sa méconnaissance de la législation étrangère sur la protection des données personnelles et/ou de l'absence d'un tel droit à l'étranger et/ou des recours possibles – à supposer que ces derniers existent et qu'ils soient effectifs au sens de l'article 47 de la Charte et de l'article 13 de la Convention européenne des droits de l'homme -, ainsi que la multiplication des démarches et recours auprès des autorités compétentes, et sans assurance d'obtenir des décisions favorables et concordantes.

Un parallèle peut être fait avec l'arrêt *Google Inc. C. Equustek Solutions* du 28 juin 2017 où la Cour suprême du Canada a enjoint à Google d'effectuer un déréférencement global ; il y était question de droits de propriété intellectuelle et de vente illégale de biens sur Internet.⁴¹ Dans cette affaire, la Cour a statué comme suit :

« Lorsqu'il faut assurer l'efficacité de l'injonction, un tribunal peut accorder une injonction dictant une conduite à adopter n'importe où dans le monde. Le problème en l'espèce se pose en ligne et à l'échelle mondiale. L'Internet n'a pas de frontières — son habitat naturel est mondial. La seule façon de s'assurer que l'injonction interlocutoire atteint son objectif est de la faire appliquer là où Google exerce ses activités, c'est-à-dire mondialement. Si l'injonction se

³⁹ CJUE, C-182/15, *Aleksei Petruhhin*, 6 septembre 2016.

⁴⁰ Conclusions, A. Bretonneau, affaire n° 399922 *Google Inc.*

⁴¹ Cour suprême du Canada, *Google Inc. C. Equustek Solutions Inc.*, 2017 CSC 34, 28 juin 2017.

limitait au Canada seulement ou à google.ca, la réparation ne pourrait pas empêcher comme il se doit le préjudice irréparable, car les acheteurs à l'extérieur du Canada pourraient facilement continuer à acheter des produits sur les sites Web de D et les acheteurs canadiens pourraient trouver ces sites même si ceux-ci ont été délistés de google.ca.

L'argument de Google selon lequel une injonction mondiale contrevient au principe de la courtoisie internationale parce qu'il est possible que l'ordonnance ne puisse pas être accordée dans un autre pays ou que Google viole les lois de ce pays en se conformant à celle-ci est théorique. Si Google dispose d'éléments de preuve démontrant que, pour se conformer à une telle injonction, elle doit contrevenir aux lois d'un autre pays, et notamment porter atteinte à la liberté d'expression, elle peut toujours demander aux tribunaux de la Colombie-Britannique de modifier l'ordonnance interlocutoire en conséquence. Jusqu'à maintenant, Google n'a pas présenté une telle demande. En l'absence d'un fondement de preuve, et compte tenu du droit de Google de demander une ordonnance de rectification, il n'est pas équitable de refuser d'accorder à E la portée extraterritoriale dont elle a besoin pour rendre la réparation efficace, ou même de lui imposer le fardeau de démontrer où — pays par pays — une telle ordonnance est légalement autorisée. [accents ajoutés] »

L'effectivité du déréférencement se pose avec davantage d'acuité pour les enfants et les adolescents, qui, en raison de leur vulnérabilité et de leur manque de discernement, doivent recevoir dans le monde numérique une protection continue qui ne saurait se limiter aux frontières de l'Europe.

En 2012, au titre de sa mission de protection des droits de l'enfant, le Défenseur des droits a consacré son rapport annuel au numérique « *Enfants et Ecrans : grandir dans le monde numérique* ». ⁴² Il y préconisait déjà la consécration d'un droit au déréférencement effectif, soulignant qu'un responsable de traitement de données personnelles n'acquiert en aucun cas la propriété des données de la personne concernée, mais la « responsabilité » de la gestion et de la conservation de ces données. Selon le sociologue, D. Boyd, l'absence de maîtrise des enfants de l'environnement numérique fait naître un besoin de protection réel. ⁴³

Cette protection s'impose pour plusieurs raisons : - l'intense exposition des enfants et adolescents sur Internet, lesquels n'ont pas conscience des risques liés à la mise en ligne de leurs données personnelles (divulgaration de données, usurpation d'identité, cyber-harcèlement, etc.) ; - la capacité limitée de l'enfant à se préserver des risques pour sa vie privée et celle des autres ; - la nécessité de permettre à l'enfant d'adapter sa vie numérique à l'évolution de sa personnalité ; et - la continuité de la vie numérique de l'enfant, et par la suite de l'adulte, et la nécessité que celui-ci puisse corriger les éventuelles erreurs du passé.

Consciente de l'effet amplificateur d'Internet, la CEDH considère que les droits des mineurs ou des jeunes sont à protéger en toutes circonstances, compte tenu de leur vulnérabilité physique et psychique, et ce d'autant plus qu'il leur sera facile d'accéder à des données en libre accès sur Internet ou d'être la cible d'abus sur Internet. ⁴⁴ Dans une affaire concernant un mineur de 12 ans ayant fait l'objet d'une annonce à caractère sexuel sur un site de rencontres par Internet, la CEDH rappelait que lorsque le bien-être physique et moral des enfants est menacé, comme sur Internet, l'Etat a l'obligation d'adopter un cadre normatif protégeant cette population vulnérable et la mettant l'abri d'ingérences dans des aspects essentiels de sa vie privée. ⁴⁵ Dans une autre affaire, *Aleksey Ovchinnikov c. Russie*, la Cour a estimé que la mention répétée par la presse de l'identité d'un mineur impliqué dans un incident violent, qui n'a pas été poursuivi pénalement en raison de son jeune âge, était préjudiciable à son développement moral et psychologique, et à sa vie privée. Le droit de la presse d'informer sur des infractions pénales graves devait donc céder ici face au droit du mineur à une protection effective de sa vie privée. ⁴⁶

⁴² https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/ddd_ra_e_2012.pdf.

⁴³ Conseil d'Etat, Etude annuelle de 2014, Le numérique et les droits fondamentaux, p.69.

⁴⁴ CEDH, Internet : la jurisprudence de la Cour européenne des droits de l'homme, juin 2015.

⁴⁵ CEDH, *K.U. c. Finlande*, no 2872/02, CEDH 2008.

⁴⁶ CEDH, *Aleksey Ovchinnikov c. Russie*, no 24061/04, 16 décembre 2010.

Le Règlement général sur la protection des données 2016/679 (« RGPD ») qui garantit un droit à l'oubli à l'article 17, prévoit désormais une protection spécifique pour les enfants : « *Les 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 (...)* »⁴⁷ Quant au droit à l'oubli, le Règlement dispose en son considérant 65 que « *ce droit est pertinent, en particulier, lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet. La personne concernée devrait pouvoir exercer ce droit nonobstant le fait qu'elle n'est plus un enfant.* » En 2016, la France a adopté des dispositions similaires en modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.⁴⁸

En tout état de cause, une protection renforcée doit être garantie aux enfants, conformément à ce qu'imposent le droit européen et la Convention relative aux droits de l'enfant, et elle implique que les droits prévus par la Directive 95/46/CE et la Loi Informatique et Libertés puissent être exercés et effectifs.

Dans une résolution du 20 novembre 2012 « Protéger les enfants dans le monde numérique », le Parlement européen soulignait également les risques d'Internet pour les enfants : « *considérant que la présence sur internet d'informations et de données à caractère personnel concernant les mineurs peut entraîner une utilisation illicite et porter atteinte à la dignité de ces derniers, en causant des préjudices considérables à leur identité, à leur conception morale et à leur insertion sociale, notamment parce que ces contenus peuvent finir entre les mains de personnes mal intentionnées* ». Le Parlement s'est félicité de l'adoption dans le RGPD de dispositions spécifiques relatives aux enfants ; cependant, il rappelle que ces dispositions doivent être pleinement opérationnelles afin d'assurer aux enfants une protection renforcée.⁴⁹

Dans le contexte du numérique, mettre en œuvre le déréférencement de manière globale s'avère être la voie la plus efficiente en matière de protection des données personnelles.

S'agissant de la technique consistant à mettre en œuvre le déréférencement en supprimant les liens litigieux des résultats de recherche sur l'ensemble des extensions nationales du moteur de recherche des Etats membres de l'Union européenne, elle s'avère insuffisante, comme cela a déjà été démontré.⁵⁰ Quant à la technique du géoblocage (« geographic filtering ») qui ne peut être envisagée, selon le Conseil d'Etat, comme complément à la technique précitée, elle n'apparaît pas entièrement satisfaisante au regard des exigences posées par la Directive 95/46/CE et l'arrêt *Google Spain*.⁵¹ Elle peut en effet être contournée en utilisant d'autres méthodes (par exemple, se connecter depuis une adresse IP identifiée comme « non européenne », utiliser un réseau privé virtuel (VPN), ...).

Cependant, outre ces possibilités de contournement, l'objectif recherché par l'auteur de la demande de déréférencement est que l'information référencée ne soit plus visible de l'ensemble des internautes quel que soit l'endroit où ils se trouvent. La Cour de justice relevait avec justesse : « *cette activité des moteurs de recherche joue un rôle décisif dans la diffusion globale desdites données en ce qu'elle rend celles-ci accessibles à tout internaute effectuant une recherche à partir du nom de la personne concernée, y compris aux internautes qui,*

⁴⁷ RGPD, Cons. 58.

⁴⁸ Article 40 de la loi.

⁴⁹ Résolution du Parlement européen du 20 novembre 2012 sur la protection des enfants dans le monde numérique (2012/2068(INI)).

⁵⁰ Voir, par exemple, B. van Alsenoy et M. Koekoek, *The extra-territorial reach of the EU's "right to be forgotten"*, Ku Leuven Center for IT & IP Law, 2015.

⁵¹ O. Tambou, *Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déréférencement*, HAL ; Voir également, B. van Alsenoy et M. Koekoek, précité.

*autrement, n'auraient pas trouvé la page web sur laquelle ces mêmes données sont publiées [accent ajouté] ».*⁵² Le déréférencement global serait conforme à l'objectif poursuivi par la directive 95/46/CE : garantir l'effectivité d'une protection pleine et entière des données personnelles, sans discontinuité.

Cette attente serait d'autant plus légitime dans certaines situations. Par exemple, un individu, à la tête d'une société française, exportant des produits dans le monde entier, demande un déréférencement afin que n'apparaissent plus dans la liste des résultats – quand on « googlise » son nom et son prénom - des informations sur la procédure de liquidation judiciaire dont a fait l'objet sa précédente société une dizaine d'années plus tôt. Manifestement, ces données ne sont plus pertinentes au regard de la Directive 95/46/CE et sont susceptibles de nuire aux activités de sa société ; cette personne est donc légitimement en droit d'obtenir un déréférencement qui soit effectif au-delà des frontières de l'Union européenne, où sa société exporte. On pourrait arguer de cette même légitimité dans les situations suivantes : une personne inconnue du grand public qui a été pénalement poursuivie mais qui a fait l'objet d'une décision de non-lieu ou de relaxe, ou encore qui a été victime de « revenge porn » sur Internet.

La Cour devra donc trouver un équilibre permettant de concilier plusieurs intérêts : l'effectivité du droit au déréférencement et l'objectif poursuivi par la Directive 95/46/CE, à savoir garantir une protection élevée des données personnelles aux personnes se trouvant sur le territoire de l'Union européenne, le respect des principes de souveraineté et de territorialité ainsi que la liberté d'accès à l'information.

Ainsi, la Cour de justice devra déterminer la portée du droit au déréférencement qu'elle a consacré dans l'arrêt *Google Spain*, de telle manière à ce que son effectivité et le niveau élevé de protection poursuivi par la Directive 95/46/CE soient garantis.

Telles sont les observations que le Défenseur des droits entend porter à la connaissance et soumettre à l'appréciation de la Cour de justice de l'Union européenne.

Le Défenseur des droits

Jacques TOUBON

⁵² CJUE, arrêt *Google Spain*, § 36.